(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－173381
（P2003－173381A）
(43)公開日　平成15年６月20日(2003.6.20)

(51)Int.Cl.'		識別記号	F I		テーマコード'(参考)
Ｇ０６Ｆ	17/60	１４２	Ｇ０６Ｆ 17/60	１４２	５Ｂ０１７
		３０２		３０２Ｅ	５Ｂ０８５
	12/14	３２０	12/14	３２０Ｆ	５Ｊ１０４
	15/00	３３０	15/00	３３０Ｂ	
				３３０Ｚ	

審査請求　未請求　請求項の数22　ＯＬ　（全 60 頁）　最終頁に続く

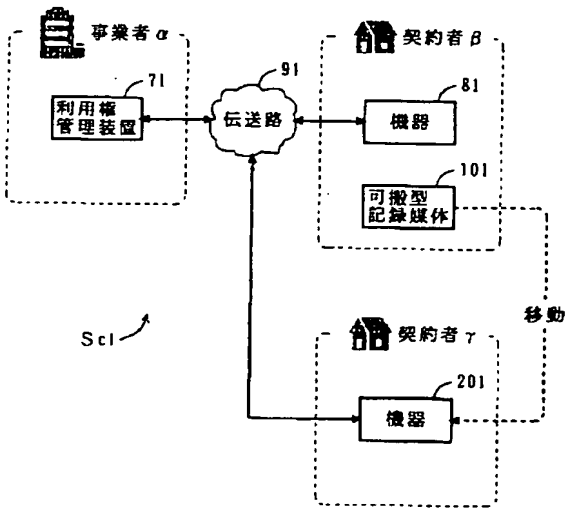
(21)出願番号　特願2002－154341(P2002－154341)
(22)出願日　平成14年５月28日(2002.5.28)
(31)優先権主張番号　特願2001－160290(P2001－160290)
(32)優先日　平成13年５月29日(2001.5.29)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2001－224413(P2001－224413)
(32)優先日　平成13年７月25日(2001.7.25)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2001－291593(P2001－291593)
(32)優先日　平成13年９月25日(2001.9.25)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　大穂　雅博
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　上坂　靖
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100098291
弁理士　小笠原　史朗

最終頁に続く

(54)【発明の名称】　利用権管理装置

(57)【要約】
【課題】　他者の機器上で、自分の利用権情報を使って、コンテンツデータを利用可能な利用権管理装置を提供すること
【解決手段】　契約者γの機器２０１は、契約者βの可搬型記録媒体１０１内のメディア識別子を使って、コンテンツデータの利用許可を受けるための発行要求を生成し、利用権管理装置７１に送信する。利用権管理装置７１は、契約者βに与えられたコンテンツデータの利用権情報を管理し、当該利用権情報と、発行要求とを使って、可搬型記録媒体１０１にコンテンツデータの利用を許可する利用許可情報を生成する。さらに、利用権管理装置７１は、利用許可情報に基づいて、可搬型記録媒体１０１に接続された機器におけるコンテンツデータの利用を制御するライセンス情報を生成して、機器２０１に送信する。機器２０１は、ライセンス情報を処理して、コンテンツデータの利用を制御する。



1

【特許請求の範囲】

【請求項１】　複数の機器がコンテンツデータを利用するための権利を表す利用権情報を管理するための装置であって、

前記複数の機器に割り当てられる利用権情報を含む利用権データベース（以下、利用権ＤＢと称する）と、

各前記機器からの発行要求に応答して、前記利用権ＤＢに含まれる利用権情報を使って、発行要求を送信した機器に対するコンテンツデータの利用許可を示す利用許可情報を生成する利用権管理部と、

前記利用権管理部で生成された利用許可情報を少なくとも含むライセンス情報を生成するライセンス情報生成部と、

前記ライセンス情報生成部で生成されたライセンス情報を、発行要求を送信した機器に送信する通信部とを備える、利用権管理装置。

【請求項２】　前記機器は、コンテンツデータの利用条件を少なくとも含む設定要求を送信し、

前記利用権管理部は、前記機器からの設定要求に応答して、少なくとも設定要求を送信した機器に対する利用権情報を前記利用権ＤＢに登録する、請求項１に記載の利用権管理装置。

【請求項３】　前記複数の機器は予め定められたグループに属しており、

前記利用権管理部は、前記グループに属する１台の前記機器からの設定要求に応答して、グループに属する各機器により共有される利用権情報を前記利用権ＤＢに登録する、請求項２に記載の利用権管理装置。

【請求項４】　配信対象となるコンテンツデータを蓄積するコンテンツデータベース（以下、コンテンツＤＢと称する）をさらに備え、

前記機器が送信する設定要求はさらに、取得対象のコンテンツデータを特定しており、

前記機器からの設定要求に応答して、コンテンツＤＢから、取得対象のコンテンツデータを読み出すコンテンツ管理部と、

前記コンテンツ管理部で読み出されたコンテンツデータを暗号化するコンテンツ暗号化部と、

前記コンテンツ暗号化部で暗号化されたコンテンツデータを含む送信データを生成する送信データ生成部とをさらに備え、

前記通信部はさらに、前記送信データ生成部で生成されたデータを、設定要求を送信した機器に送信する、請求項２に記載の利用権管理装置。

【請求項５】　前記コンテンツ暗号化部で暗号化されるコンテンツデータを復号するための復号鍵を含む復号鍵データベース（以下、復号鍵ＤＢと称する）をさらに備え、

前記ライセンス情報生成部は、前記復号鍵ＤＢ内の復号鍵をさらに含むライセンス情報を生成する、請求項１に記載の利用権管理装置。

2

【請求項６】　前記復号鍵ＤＢ内の復号鍵を、発行要求を送信した機器に関連する情報で暗号化する復号鍵暗号化部をさらに備え、

前記ライセンス情報生成部は、前記復号鍵暗号化部で暗号化された復号鍵をさらに含むライセンス情報を生成する、請求項５に記載の利用権管理装置。

【請求項７】　前記ライセンス情報生成部は、

前記利用権管理部で生成された利用許可情報に基づいて、ライセンス情報の改竄を防止するためのハッシュ値を生成するハッシュ値生成部と、

前記ハッシュ値生成部で生成されたハッシュ値を、前記利用権管理部で生成された利用許可情報に付加して、ライセンス情報を組み立てるライセンス情報組立部とを含む、請求項１に記載の利用権管理装置。

【請求項８】　前記利用権管理部は、発行要求の送信元となる機器のために利用許可情報を生成できない場合には、利用拒否情報を生成し、

前記通信部はさらに、前記利用権管理部で生成された利用拒否情報を、発行要求の送信元のなる機器に送信する、請求項１に記載の利用権管理装置。

【請求項９】　予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報ＤＢと称する）と、

前記ユーザ情報ＤＢに未登録の機器識別子を有する機器からの登録要求に応答して、受信登録要求に含まれる未登録の機器識別子を前記ユーザ情報ＤＢに登録するユーザ情報管理部とをさらに備える、請求項１に記載の利用権管理装置。

【請求項１０】　前記ユーザ情報管理部は、１グループに登録されている機器識別子数が、予め定められた上限値以上である場合には、登録要求に応答して、前記ユーザ情報ＤＢへの登録を拒否するための登録拒否通知を生成し、

前記通信部はさらに、前記ユーザ情報管理部で生成された登録拒否通知を、登録要求の送信元となる機器に送信する、請求項９に記載の利用権管理装置。

【請求項１１】　予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報ＤＢと称する）をさらに備え、

前記ユーザ情報ＤＢに登録済の機器は、自身の機器識別子を登録対象識別子として少なくとも含む仮登録要求を送信し、

受信仮登録要求に含まれる登録対象識別子を前記ユーザ情報ＤＢに仮登録するユーザ情報管理部をさらに備え、

前記ユーザ情報ＤＢに未登録の機器は、登録対象識別子と、仮登録要求の送信元となった機器の機器識別子である登録済識別子とを少なくとも含む本登録要求を送信し、

前記ユーザ情報管理部は、受信本登録要求に含まれる登録対象識別子および登録済識別子に基づいて、前記ユーザ情報ＤＢに仮登録された登録対象識別子を本登録する、請求項１に記載の利用権管理装置。

【請求項１２】　予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報ＤＢと称する）をさらに備え、

前記ユーザ情報ＤＢに未登録の機器は、自身の機器識別子を登録対象識別子として含み、さらに、登録済の機器識別子を含むパスワード要求を送信し、

受信パスワード要求に含まれる登録対象識別子を前記ユーザ情報ＤＢに仮登録し、さらに、未登録の機器に対するパスワードを発行するユーザ情報管理部をさらに備え、

前記ユーザ情報ＤＢに未登録の機器は、登録対象識別子と、前記ユーザ情報管理部により発行されたパスワードとを含む登録要求を送信し、

前記ユーザ情報管理部は、受信登録要求に含まれるパスワードと登録対象識別子とに基づいて、前記ユーザ情報ＤＢに仮登録された登録対象識別子を本登録する、請求項１に記載の利用権管理装置。

【請求項１３】　予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報ＤＢと称する）をさらに備え、

前記ユーザ情報ＤＢに未登録の機器は、自身の機器識別子を登録対象識別子として少なくとも含む第１の登録要求を、ユーザ情報ＤＢに登録済の機器に送信し、

前記ユーザ情報ＤＢに登録済の機器は、自身の機器識別子を登録済識別子として含み、さらに、受信した第１の登録要求に含まれる登録対象識別子を含む第２の登録要求を送信し、

受信した第２の登録要求に含まれる登録対象識別子を前記ユーザ情報ＤＢに登録するユーザ情報管理部をさらに備える、請求項１に記載の利用権管理装置。

【請求項１４】　前記利用権ＤＢには、利用権情報と、その利用権情報を利用可能な機器の機器識別子とが登録されており、

予め定められたグループに属する機器のそれぞれを一意に特定する機器識別子からなるユーザ情報データベース（以下、ユーザ情報ＤＢと称する）と、

各前記機器からの削除要求に応答して、前記ユーザ情報ＤＢおよび前記利用権ＤＢから機器識別子を削除する機器識別子削除部とをさらに備える、請求項１に記載の利用権管理装置。

【請求項１５】　前記複数の機器は予め定められたグループに属しており、

前記利用権管理部は、

前記グループに属する第１の機器からの設定要求に応答して、設定要求の送信元となる第１の機器の利用権情報を前記利用権ＤＢに登録し、

前記グループに属する第２の機器からの設定要求に応答して、設定要求の送信元となる第２の機器を、第１の機器の利用権情報と共有可能に前記利用権ＤＢに登録する、請求項２に記載の利用権管理装置。

【請求項１６】　伝送路を通じて接続された利用権管理装置から、ライセンス情報の提供を受ける機器であって、

前記機器は、

自身を一意に特定するメディア識別子を格納する可搬型記録媒体をデータ通信可能に接続するインターフェイスと、

前記インターフェイスに接続された可搬型記録媒体からメディア識別子を取り出す識別子抽出部と、

前記識別子抽出部から受け取るメディア識別子を使って、コンテンツデータの利用許可を受けるために必要な発行要求を生成する発行要求生成部と、

前記発行要求生成部から受け取る発行要求を、前記伝送路を通じて、前記利用権管理装置に送信する第１の通信部とを備え、

前記利用権管理装置は、

前記可搬型記録媒体に与えられたコンテンツデータの利用権情報を管理しており、前記機器からの発行要求に応答して、前記可搬型記録媒体が接続された機器におけるコンテンツデータの利用を制御するためのライセンス情報を生成して送信し、

前記機器はさらに、

前記利用権管理装置からのライセンス情報を処理して、コンテンツデータの利用を制御するライセンス情報処理部とを備える、機器。

【請求項１７】　前記利用権管理装置は、前記機器がコンテンツデータを利用するための最低限度の利用許可情報を生成する利用権管理部を備える、請求項１６に記載の機器。

【請求項１８】　前記利用権管理装置は、

ライセンス情報を生成するために、前記利用権管理部で生成された利用許可情報に基づいて、第１のハッシュ値を生成する第１のハッシュ値生成部と、

前記第１のハッシュ値生成部から受け取る第１のハッシュ値を、前記利用権管理部から受け取る利用許可情報に付加して、ライセンス情報を組み立てるライセンス情報組立部とを含む、請求項１７に記載の機器。

【請求項１９】　前記ライセンス情報処理部は、

受信ライセンス情報に含まれる利用許可情報に基づいて、第２のハッシュ値を生成する第２のハッシュ値生成部と、

前記第１の通信部から受け取るライセンス情報に含まれる第１のハッシュ値と、前記第２のハッシュ値生成部から受け取る第２のハッシュ値とに基づいて、

前記第１の通信部から受け取るライセンス情報に含まれる利用許可情報が改竄されているか否かを判定する改竄判定部とを含む、請求項１８に記載の機器。

【請求項２０】　前記コンテンツデータは、前記機器に、予め定められた暗号鍵で暗号化された状態で配信され、

前記ライセンス情報組立部はさらに、前記利用権管理部から受け取る発行要求からメディア識別子を取り出し、

前記利用権管理装置は、

前記暗号鍵で暗号化されたコンテンツデータを復号可能な復号鍵を管理する復号鍵管理部と、

前記復号鍵管理部で管理される復号鍵を、前記ライセンス情報組立部により取り出されたメディア識別子で暗号化する復号鍵暗号化部とをさらに備え、

前記ライセンス情報組立部はさらに、前記復号鍵暗号化部から受け取る暗号化された復号鍵を、前記利用権管理部から受け取る利用許可情報に付加して、ライセンス情報を組み立てる、請求項１８に記載の機器。

【請求項２１】　前記ライセンス情報処理部は、前記識別子抽出部から受け取るメディア識別子を使って、前記第１の通信部から受け取るライセンス情報に含まれる暗号化された復号鍵を復号する復号鍵復号部をさらに備える、請求項２０に記載の機器。

【請求項２２】　自身に割り当てられた機器識別子を格納するための機器識別子格納部をさらに備え、

前記識別子抽出部は、ユーザの操作に応じて、前記インターフェイスに接続された可搬型記録媒体からメディア識別子を取り出すか、前記機器識別子格納部から機器識別子を取り出すかを決定する、請求項１６に記載の機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、利用権管理装置に関し、より特定的には、コンテンツデータに関連する権利を管理する利用権管理装置に関する。

【０００２】

【従来の技術】近年、ネットワークのブロードバンド化および常時接続環境により、コンテンツ配信システムが身近なものになりつつある。また、このようなコンテンツ配信システムの普及には、コンテンツデータに関連する権利の保護が重要であることから、従来から、様々な権利管理技術の研究および開発がなされている。ここで、本願明細書では、著作権または販売権のようなコンテンツデータに関連する権利を、デジタルライツと称する。以下、従来の権利管理技術を組み込んだコンテンツ情報配信システムについて説明する。

【０００３】従来のコンテンツ配信システムには、コンテンツ配信装置と、パーソナルコンピュータ（以下、ＰＣと略記する）とが、インターネットに代表されるネットワークにより、データ通信可能に接続される。コンテンツ配信装置は、コンテンツデータ、コンテンツ復号鍵および利用条件データの組みを少なくとも１つ格納している。コンテンツデータは、例えば、音楽に代表されるコンテンツを表すデジタルデータであり、予め定められた方式で暗号化される。コンテンツ復号鍵は、暗号化されたコンテンツデータを復号するための鍵である。利用条件データは、上述のコンテンツデータの利用可能な条件（以下、利用条件と称する）を表すデータである。利用条件としては、コンテンツデータの利用回数が代表的である。ＰＣは、上述のコンテンツデータをコンテンツ配信装置から取得し、さらに、取得したコンテンツデータを利用するために必要なコンピュータプログラム（以下、単にプログラムと称する）を格納している。

【０００４】以上のコンテンツ配信システムでは、以下のようにして、コンテンツデータが配信される。まず、ＰＣは、予め格納されているプログラムを実行して、コンテンツデータの配信をコンテンツ配信装置に要求する。コンテンツデータの要求は、一般的に、コンテンツ特定情報および端末固有情報を、ＰＣがネットワークを介してコンテンツ配信装置に送信することで行われる。コンテンツ特定情報は、上述のコンテンツデータを一意に特定する情報である。端末固有情報は、ＰＣにより予め保持されており、上述のコンテンツデータの要求元であるＰＣを一意に特定可能な情報である。

【０００５】コンテンツ配信装置は、ＰＣからの要求に応答して、上述のコンテンツ復号鍵を、今回受信した端末固有情報を使って暗号化する。その後、コンテンツ配信装置は、上述の暗号化されたコンテンツデータと、端末固有情報で暗号化されたコンテンツ復号鍵と、利用条件データとをＰＣに送信する。ＰＣは、コンテンツ配信装置により配信されたコンテンツデータ、コンテンツ復号鍵および利用条件データを受信し、内部に備える記憶装置に格納する。

【０００６】以上の格納後、ＰＣのユーザは、コンテンツデータを復号することで、それが表すコンテンツを出力可能な状態になる。実際にコンテンツを出力するまでには、ユーザは最初に、その旨をＰＣに指示する。この指示に応答して、ＰＣは、以下のように動作する。ＰＣは、記憶装置内の利用条件データにより表される利用条件に、今回の利用が合致しているか否かを判定する。ＰＣは、利用条件に合致する場合に限り、以下の処理を実行する。次に、記憶装置内のコンテンツ復号鍵は暗号化されているので、ＰＣは、自身が保持する端末固有情報を使って、当該コンテンツ復号鍵を復号する。さらに、記憶装置内のコンテンツデータもまた上述のように暗号化されているので、ＰＣは、復号したコンテンツ復号鍵を使って、当該コンテンツデータを復号した後、それが表すコンテンツを再生し出力する。

【０００７】以上のコンテンツ配信システムでは、権利管理技術としてのＤＲＭ(Digital Rights Management)

により、デジタルライツが保護されている。ＤＲＭによるデジタルライツの保護は、以下の３つの技術により実現される。第１の保護技術では、コンテンツ配信装置は、暗号化されたコンテンツデータと、端末固有情報で暗号化されたコンテンツ復号鍵を送信する。ここで、コンテンツ復号鍵は、コンテンツデータを要求したＰＣ以外では復号できない。それゆえ、たとえ、暗号化されたコンテンツデータが他のＰＣに転送されたとしても、他のＰＣは、コンテンツ復号鍵の暗号を解くことができず、その結果、コンテンツデータを再生することができない。以上のことから、ＤＲＭでは、コンテンツ復号鍵は、唯一のＰＣに括り付けられると言える。これにより、デジタルライツが保護される。

【０００８】第２の保護技術は耐タンパ技術である。つまり、ＰＣには、各暗号を解くための復号プログラムが必要となるが、当該復号プログラムの解析は、上述の耐タンパ技術により防止される。これによっても、デジタルライツが保護される。

【０００９】第３に、上述したように、従来のコンテンツ配信システムでは、コンテンツ配信装置は、利用条件データをＰＣに送信する。ＰＣは、受信した利用条件データを管理する。そして、ＰＣは、コンテンツデータの利用毎に、自身が管理する利用条件データが表す利用条件をチェックし、今回の利用が利用条件に合致していない場合には、それ以降の処理を行わない。これによっても、デジタルライツが保護される。

【００１０】

【発明が解決しようとする課題】近年、セットトップボックス、テレビジョン受像機、音楽再生機およびゲーム機器に代表されるＰＣ以外の民生機器にもネットワーク接続機能が付加されるようになってきた。これによって、民生機器が上述のコンテンツ配信装置からコンテンツデータを受信できるようになり、さらには、複数の民生機器の間でデータ通信ができるようになってきた。以上のことから、民生機器にも権利管理技術が組み込まれることが望まれる。しかしながら、上述のＤＲＭのような権利管理技術を民生機器に組み込むことは、以下の問題点を想定できるため得策ではない。

【００１１】第１に、コンテンツ復号鍵は、唯一のＰＣに括り付けられるため、ＰＣおよび他の民生機器の利用者が同一であっても、他の民生機器は、そのコンテンツ復号鍵を使って、コンテンツデータを復号することができないという問題点があった。このような問題点ゆえ、利用者は、コンテンツデータを利用する際には、コンテンツ鍵を利用できるＰＣを使わなければならないため、従来の権利管理技術は、利用者にとって使い勝手の良いものではなかった。

【００１２】第２に、上述のＤＲＭには、耐タンパ技術が組み込まれ、さらに、ＰＣがコンテンツデータを再生する前に必ず、内部に格納した利用条件データに基づいて、当該コンテンツデータを利用可能か否かをチェックする。このように耐タンパ技術は上述のＰＣに大きな処理負担を強いる。しかしながら、ＰＣは、例えば、ビデオ再生、オーディオ再生またはゲームプレイ等、汎用的な用途に使えるよう、相対的に高性能なハードウェアを実装している。それゆえ、ＰＣにＤＲＭを組み込んでも、さほど問題にはならない。それに対して、民生機器に求められるのは低価格であり、さらに、民生機器は、ビデオ再生、オーディオ再生およびゲームプレイのそれぞれに特化した用途に使用されることが一般的である。以上の観点から、民生機器には、ＰＣほど高性能なハードウェアが実装されておらず、大きな処理負担を要求するＤＲＭを組み込むのは困難であるという問題点があった。

【００１３】それ故に、本発明の第１の目的は、複数の民生機器が共通のデジタルライツを共有できる権利管理技術を提供することである。また、本発明の第２の目的は、民生機器に適した権利管理技術を提供することである。

【００１４】

【課題を解決するための手段および発明の効果】上記第１の目的を達成するために、本願の第１の発明は、複数の機器がコンテンツデータを利用するための権利を表す利用権情報を管理するための装置であって、複数の機器に割り当てられる利用権情報を含む利用権データベース（以下、利用権ＤＢと称する）と、各機器からの発行要求に応答して、利用権ＤＢに含まれる利用権情報を使って、発行要求を送信した機器に対するコンテンツデータの利用許可を示す利用許可情報を生成する利用権管理部と、利用権管理部で生成された利用許可情報を少なくとも含むライセンス情報を生成するライセンス情報生成部と、ライセンス情報生成部で生成されたライセンス情報を、発行要求を送信した機器に送信する通信部とを備える。

【００１５】上記のように第１の発明によれば、利用権情報は、複数の機器に割り当てられるので、複数の機器が共通の利用権情報を共有可能な権利保護技術を提供することが可能となる。

【００１６】上記第２の目的を達成するために、本願の第２の発明は、伝送路を通じて接続された利用権管理装置から、ライセンス情報の提供を受ける機器であって、可搬型記録媒体は、自身を一意に特定するメディア識別子を格納しており、機器は、可搬型記録媒体をデータ通信可能に接続するインターフェイスと、インターフェイスに接続された可搬型記録媒体からメディア識別子を取り出す識別子抽出部と、識別子抽出部から受け取るメディア識別子を使って、コンテンツデータの利用許可を受けるために必要な発行要求を生成する発行要求生成部と、発行要求生成部から受け取る発行要求を、伝送路を通じて、利用権管理装置に送信する第１の通信部とを備

える。ここで、利用権管理装置は、可搬型記録媒体に与えられたコンテンツデータの利用権情報を管理しており、機器からの発行要求に応答して、可搬型記録媒体が接続された機器におけるコンテンツデータの利用を制御するためのライセンス情報を生成して送信する。機器はさらに、利用権管理装置からのライセンス情報を処理して、コンテンツデータの利用を制御するライセンス情報処理部とを備える。

【００１７】上記のように第２の発明によれば、コンテンツデータの利用権情報を利用権管理装置側で管理しているので、機器に、利用権情報のためにかかる処理負担を負わせる必要が無くなる。これによって、相対的に処理能力の低い機器に適した権利保護技術を提供することが可能となる。

【００１８】さらに、第２の発明によれば、機器において、識別子抽出部は、機器に接続された可搬型記録媒体から、メディア識別子を取り出す。さらに、発行要求生成部は、取り出されたメディア識別子を使って発行要求を生成することができる。これによって、可搬型記録媒体のユーザは、自分の利用権情報を使って、他者の機器上でコンテンツデータを利用することが可能となる。

【００１９】

【発明の実施の形態】「第１の実施形態」図１は、本発明の第１の実施形態に係る利用権管理装置１１を収容したライセンス情報管理システムＳａの全体構成を示すブロック図である。図１において、ライセンス情報管理システムＳａは、利用権管理装置１１と、複数の機器２１の一例として２つの機器２１ａおよび２１ｂと、伝送路３１とを備えている。利用権管理装置１１は、コンテンツ配信に関わる事業者α側に設置される。また、機器２１ａおよび２１ｂは、典型的には、事業者αとの契約に基づいてコンテンツ配信を受ける契約者βにより使用される。また、伝送路３１は、有線または無線であり、利用権管理装置１１と、機器２１ａまたは機器２１ｂとをデータ通信可能に接続する。

【００２０】次に、図２を参照して、図１の利用権管理装置１１の詳細な構成について説明する。図２において、利用権管理装置１１は、コンテンツデータベース１１１と、復号鍵データベース１１２と、ユーザ情報データベース１１３と、利用権データベース１１４と、通信部１１５と、ユーザ認証部１１６と、利用権管理部１１７と、コンテンツ管理部１１８と、コンテンツ暗号化部１１９と、送信データ生成部１２０と、ライセンス情報生成部１２１と、復号鍵管理部１２２と、復号鍵暗号化部１２３とを備えている。また、ライセンス情報生成部１２１は、より詳しくは、図３に示すように、ハッシュ値生成部１２１１と、ライセンス情報組立部１２１２とを含んでいる。

【００２１】次に、図４を参照して、図１の機器２１ａおよび２１ｂの詳細な構成について説明する。図４において、機器２１ａおよび２１ｂは、典型的には、パーソナルコンピュータ（以下、ＰＣと称する）、セットトップボックス、音楽再生機、テレビジョン受像機およびゲーム機のいずれかである。ただし、本実施形態では、便宜上、機器２１ａおよび２１ｂは、それぞれが音楽再生機能を有するＰＣおよび音楽再生機であると仮定する。この仮定下では、機器２１ａおよび２１ｂのそれぞれは少なくとも、機器識別子格納部２１１と、設定要求生成部２１２と、通信部２１３と、コンテンツ管理部２１４と、コンテンツ蓄積部２１５と、発行要求生成部２１６と、ライセンス情報処理部２１７と、コンテンツ復号部２１８と、コンテンツ再生部２１９とを備えている。また、ライセンス情報処理部２１７は、より詳しくは、図５に示すように、改竄判定部２１７１と、ハッシュ値生成部２１７２と、利用許可判定部２１７３と、復号鍵復号部２１７４とを含んでいる。

【００２２】次に、上記ライセンス情報管理システムＳａにおいて、契約者βが事業者αからコンテンツ配信を受けるために必要となる準備について説明する。この準備作業では、図２のコンテンツデータベース（以下、コンテンツＤＢと称す）１１１と、復号鍵データベース（以下、復号鍵ＤＢと称す）１１２と、ユーザ情報データベース（以下、ユーザ情報ＤＢと称す）１１３とが事業者αにより構築される。

【００２３】まず、図６（ａ）を参照して、図２のコンテンツＤＢ１１１について詳細に説明する。まず、事業者αは、契約者βに配信されるコンテンツデータＤcntを、自分で作成したり、別のコンテンツ制作者から受け取る。ここで、コンテンツデータＤcntは、機器２１ａおよび２１ｂの両方で利用可能なデータであって、例えば、テレビ番組、映画、ラジオ番組、音楽、書籍または印刷物を表す。また、コンテンツデータＤcntは、ゲームプログラムまたはアプリケーションソフトウェアであっても良い。ただし、便宜上、本実施形態では、コンテンツデータＤcntは音楽を表すデータであると仮定する。

【００２４】事業者αは、以上のようにして得たコンテンツデータＤcntのそれぞれに、コンテンツ識別子Ｉcntを割り当てる。コンテンツ識別子Ｉcntは好ましくは、本ライセンス情報管理システムＳａにおいてコンテンツデータＤcntを一意に特定する情報である。さらに、コンテンツ識別子Ｉcntは、コンテンツデータＤcntの格納場所を示すロケータでもあることが好ましい。また、以上のコンテンツデータＤcntは、デジタルライツを保護する観点から、利用権管理装置１１側で暗号化された状態で機器２１ａまたは２１ｂに配信される。そのため、事業者αは、各コンテンツデータＤcntに専用の暗号鍵Ｋｅを割り当てる。以上のコンテンツ識別子Ｉcnt、コンテンツデータＤcntおよび暗号鍵Ｋｅの組み合わせがコンテンツＤＢ１１１に蓄積される。したがっ

て、図６（ａ）に示すように、コンテンツＤＢ１１１は、コンテンツ識別子Ｉcnt、コンテンツデータＤcntおよび暗号鍵Ｋｅの組み合わせの集まりとなる。コンテンツＤＢ１１１において、コンテンツ識別子Ｉcntは特に、同じ組みのコンテンツデータＤcntを一意に特定する。また、暗号鍵Ｋｅは、同じ組みのコンテンツデータＤcntを暗号化するために使用される。

【００２５】また、本実施形態では、図示の簡素化するため、コンテンツＤＢ１１１は、コンテンツ識別子Ｉcnt、コンテンツデータＤcntおよび暗号鍵Ｋｅから構成されるとして説明するが、コンテンツデータＤcntおよび暗号鍵Ｋｅ毎のデータベースが構築されてもよい。また、コンテンツ識別子Ｉcntは、コンテンツデータＤcntのロケータであることが好ましい。このような場合、利用権管理装置１１は、機器２１ａまたは２１ｂの設定要求Ｄrraに含まれるコンテンツ識別子Ｉcntを使って、コンテンツＤＢ１１１からコンテンツデータＤcntを読み出せるので、コンテンツＤＢ１１１に、コンテンツ識別子Ｉcntを登録しておく必然性はない。

【００２６】次に、図６（ｂ）を参照して、図２の復号鍵ＤＢ１１２について詳細に説明する。上述のように、各コンテンツデータＤcntは暗号鍵Ｋｅで暗号化された状態で機器２１ａまたは２１ｂに送信される。ここで、以下の説明では、暗号鍵Ｋｅで暗号化されたコンテンツデータＤcntを、暗号済みコンテンツデータＤecntと称する。暗号済みコンテンツデータＤecntの復号のためには、暗号鍵Ｋｅに対応する復号鍵Ｋｄが、機器２１ａまたは２１ｂに提供される必要がある。この必要性から、事業者αは、コンテンツＤＢ１１１内の各暗号鍵Ｋｅに対応する復号鍵Ｋｄを準備する。ここで、復号鍵Ｋｄは、暗号鍵Ｋｅと同じビット列からなっていてもよいし、異なるビット列からなっていてもよい。以上の復号鍵Ｋｄは、上述のコンテンツ識別子Ｉcntと共に、復号鍵ＤＢ１１２に登録される。以上のことから、復号鍵ＤＢ１１２は、図６（ｂ）に示すように、コンテンツ識別子Ｉcntおよび復号鍵Ｋｄの組み合わせの集まりとなる。復号鍵ＤＢ１１２において、コンテンツ識別子Ｉcntは特に、同じ組みの復号鍵Ｋｄに割り当てられているコンテンツデータＤcntを特定する。また、復号鍵Ｋｄは、同じ組みのコンテンツ識別子Ｉcntで特定される暗号済みコンテンツデータＤecntを復号するために使用される。

【００２７】次に、図７（ａ）を参照して、図２のユーザ情報ＤＢ１１３について詳細に説明する。上述のように、契約者βは、事業者αとコンテンツ配信に係る契約を交わす。ここで、両者の契約に関しては、契約者βが伝送路３１を通じて事業者αと行ってもよいし、他の形態で行ってもよい。この契約に基づいて、事業者αは、契約者βが所有する複数の機器２１（つまり、機器２１ａおよび２１ｂ）のそれぞれに機器識別子Ｉdvを割り当てる。ここで、図１に示すように、本実施形態では、機器２１ａと２１ｂとが例示されているから、事業者αは、それぞれの機器識別子ＩdvとしてIdva およびＩdvbを割り当てる。機器識別子Ｉdva およびＩdvbは、ライセンス情報管理システムＳａにおいて、契約者β側の機器２１ａおよび２１ｂを一意に特定する。以上の機器識別子Ｉdva およびＩdvbが、ユーザ情報ＤＢ１１３に登録される。さらに、事業者αは、契約者βおよびその関係者が、機器２１ａおよび２１ｂのいずれを使っても、コンテンツデータＤcntを利用できるように、グループ識別子Ｉgpを、契約者βとの契約に割り当てる。ここで、契約者βおよびその関係者を包括的に述べることができるように、これらをユーザβと称する。以上の機器識別子Ｉdva およびＩdvbと、グループ識別子Ｉgpとを使って、事業者αは、ユーザ情報ＤＢ１１３を構築する。

【００２８】より具体的には、ユーザ情報ＤＢ１１３は、図７（ａ）に示すように、複数の契約者レコードＲcsの集まりである。契約者レコードＲcsは、１契約毎に作成され、典型的には、グループ識別子Ｉgpと、機器識別子数Ｎdvと、複数の機器識別子Ｉdvとを含む。グループ識別子Ｉgpは、契約者レコードＲcsに含まれる複数の機器識別子Ｉdvが同一のグループに属することを特定する。機器識別子数Ｎdvは、グループ識別子Ｉgpで特定されるグループに属する機器２１の数を示す。各機器識別子Ｉdvは、グループ識別子Ｉgpで特定されるグループに属する各機器２１を特定する。以上の契約者レコードＲcsにより、利用権管理装置１１は、複数の機器２１が同一グループに属することを把握することができる。なお、もし、契約者が１台の機器２１しか使わない場合には、契約者レコードＲcsは、それに割り当てられた機器識別子Ｉdvのみを含んでいれば良い。

【００２９】ここで図４を再度参照する。事業者αにより割り当てられた機器識別子Ｉdvaおよびｉdvbはさらに、ユーザβ側の機器２１ａおよび２１ｂにおける機器識別子格納部２１１に設定される。ここで注意を要するのは、図４では機器識別子Ｉdva およびＩdvbの双方が機器識別子格納部２１１に格納されるように見えるが、そうではなく、機器２１ａの機器識別子格納部２１１には機器識別子Ｉdva が設定され、機器２１ｂの機器識別子格納部２１１には機器識別子Ｉdvbが設定される。また、以上の機器識別子Ｉdva およびＩdvbの設定に関しては、例えば、事業者αがユーザβ側の機器２１ａまたは２１ｂを操作して設定する。また、他にも、事業者α側が、伝送路３１を通じて、契約者βに割り当てた機器識別子Ｉdva またはＩdvbを機器２１ａまたは２１ｂに送信し、それぞれが、受信した機器識別子Ｉdva またはＩdvbを、それぞれの機器識別子格納部２１１に自動的に設定するようにしてもよい。さらに、以上の機器識別子Ｉdva およびＩdvbは、機器２１ａまたは２１ｂの工

場出荷時に、それぞれの機器識別子格納部２１１に設定されていてもよい。このような場合、契約者βは、契約時に、機器２１ａおよび２１ｂに設定されている機器識別子Ｉdva およびＩdvb を事業者αに告知する。事業者αは、告知された機器識別子Ｉdva およびＩdvb を使って、ユーザ情報ＤＢ１１３を構築する。

【００３０】また、図７（ｂ）には、利用権データベース１１４が示されているが、これについては後述する。

【００３１】以上の準備が終了すると、機器２１ａおよび２１ｂの一方は、ユーザβの操作に従って、利用権管理装置１１に対して、コンテンツデータＤcnt の利用権を設定することや、コンテンツデータＤcnt を取得することが可能となる。以下、図８を参照して、コンテンツデータＤcnt の利用権設定および取得時における、機器２１ａおよび利用権管理装置１１の間のデータ通信について説明する。まず、ユーザβは、機器２１ａを操作して、利用権管理装置１１にアクセスし、コンテンツＤＢ１１１内のコンテンツデータＤcnt から、今回取得したいもののコンテンツ識別子Ｉcnt を特定する。以降の説明において、今回指定されたコンテンツデータＤcnt を、取得対象コンテンツデータＤcnt と称する。さらに、ユーザβは、取得対象コンテンツデータＤcnt を利用する際の利用条件Ｃcnt を指定する。

【００３２】以下、利用条件Ｃcnt について、より詳細に説明する。利用条件Ｃcnt は、どのような条件で、機器２１ａがコンテンツデータＤcnt の利用権の設定を要求するのかを示す情報である。コンテンツデータＤcnt が音楽を表す場合、利用条件Ｃcnt としては、有効期間、再生回数、最大連続再生時間、総再生時間または再生品質が代表的である。また、利用条件Ｃcnt は、有効期間、再生回数、最大連続再生時間、総再生時間および再生品質の内、２つ以上の組み合わせであってもよい。利用条件Ｃcnt としての有効期間は、例えば、２００１年６月１日から２００１年８月３１日までと設定され、設定された期間に限り、機器２１ａは、コンテンツデータＤcnt を再生できる。再生回数は、例えば、５回と設定され、設定された回数に限り、機器２１ａは、コンテンツデータＤcnt を再生できる。最大連続再生時間は、例えば、１０秒と設定され、１回の再生において設定された時間までであれば、機器２１ａは、コンテンツデータＤcnt を再生できる。このような最大連続再生時間は、音楽のプロモーションに特に有効である。総再生時間は、例えば、１０時間と設定され、設定された時間の範囲内であれば、機器２１ａは、コンテンツデータＤcnt を自由に再生できる。再生品質は、例えば、ＣＤ(Compact Disc)の品質と設定され、機器２１ａは、設定された再生品質でコンテンツデータＤcnt を再生できる。

【００３３】なお、上述では、コンテンツデータＤcnt が音楽を表す場合に設定されうる利用条件Ｃcnt について説明した。しかし、上述のみに限らず、利用条件Ｃcnt は、コンテンツデータＤcnt が表す内容に応じて、適切に設定されることが好ましい。また、便宜上、本実施形態では、利用条件Ｃcnt は、コンテンツデータＤcnt の再生回数であるとして、以下の説明を続ける。

【００３４】上述したように、ユーザβは、機器２１ａを操作して、コンテンツ識別子Ｉcnt および利用条件Ｃcnt を指定する。この指定に応答して、機器２１ａは、図９（ａ）に示す設定要求Ｄrra を生成し、利用権管理装置１１に送信する（図８；ステップＳ１１）。設定要求Ｄrra は、取得対象コンテンツデータＤcnt の利用権設定を利用権管理装置１１に要求するための情報であるが、本実施形態ではさらに、取得対象コンテンツデータＤcnt の配信を利用権管理装置１１に要求するための情報でもある。ステップＳ１１をより具体的に説明すると、まず、設定要求生成部２１２（図４参照）は、ユーザβが指定したコンテンツ識別子Ｉcnt および利用条件Ｃcnt を受け取る。また、設定要求生成部２１２は、機器識別子格納部２１１から機器識別子Ｉdva を受け取る。その後、設定要求生成部２１２は、以上の機器識別子Ｉdva 、コンテンツ識別子Ｉcnt および利用条件Ｃcnt に、予め保持する設定要求識別子Ｉrrを付加して、設定要求Ｄrra （図９（ａ）参照）を生成する。ここで、設定要求識別子Ｉrrは、利用権管理装置１１が設定要求Ｄrra を特定するために使用される。設定要求生成部２１２は、以上の設定要求Ｄrra を通信部２１３に渡す。通信部２１３は、受け取った設定要求Ｄrra を、伝送路３１を通じて、利用権管理装置１１に送信する。

【００３５】利用権管理装置１１（図２参照）において、通信部１１５は、伝送路３１を通じて送信されてくる設定要求Ｄrra を受信して、ユーザ認証部１１６に渡す。ユーザ認証部１１６は、設定要求Ｄrra を受け取ると、その送信元の機器２１ａが契約ユーザβの物であるか否かを判定するためのユーザ認証処理を行う（図８；ステップＳ１２）。より具体的には、ユーザ認証部１１６は、上述のユーザ情報ＤＢ１１３（図７（ａ）参照）にアクセスし、受け取った設定要求Ｄrra 内の機器識別子Ｉdva に一致するものが、当該ユーザ情報ＤＢ１１３に登録されているか否かを確認する。ユーザ認証部１１６は、ユーザ情報ＤＢ１１３に一致するものが登録されている場合に限り、今回設定要求Ｄrra が、ユーザβの機器２１ａから送信されてきたものであると認証する。ユーザ認証部１１６は、以上のユーザ認証が終了すると、受け取った設定要求Ｄrra を利用権管理部１１７に渡す。

【００３６】なお、契約ユーザβ以外からの設定要求Ｄrra を受け取った場合、ユーザ認証部１１６は、ユーザ認証に失敗する。この場合、ユーザ認証部１１６は、受信設定要求Ｄrra を利用権管理部１１７に渡すことなく廃棄する。

【００３７】利用権管理部１１７は、ユーザ認証部１１

６からの受信情報に設定されている設定要求識別子Ｉrrを判定することで、今回の受信情報が設定要求Ｄrra であることを認識する。この認識結果に従って、利用権管理部１１７（図２参照）は、利用権データベース（以下、利用権ＤＢと称する）１１４にアクセスして、利用権ＤＢ１１４への利用権登録処理を行う（ステップＳ１３）。より具体的には、利用権管理部１１７は、受信設定要求Ｄrra から機器識別子Ｉdva およびコンテンツ識別子Ｉcnt を取り出して、これらを含む利用権レコードＲrqt が利用権ＤＢ１１４（図７（ｂ）参照）に登録されているか否かを判断する（ステップＳ１３１）。今、利用権ＤＢ１１４には対象となる利用権レコードＲrqtが未登録であると仮定すると、利用権管理部１１７は、ステップＳ１３２を実行する。なお、ステップＳ１３１で利用権レコードＲrqt が登録済の場合の動作については、機器２１ｂ の動作と共に説明するため、ここではその説明を省略する。

【００３８】ステップＳ１３２において、利用権管理部１１７はまず、受信設定要求Ｄrraから機器識別子Ｉdva、コンテンツ識別子Ｉcnt および利用条件Ｃcnt を取り出した後、ユーザ情報ＤＢ１１３（図７（ａ）参照）にアクセスする。そして、利用権管理部１１７は、今回取り出した機器識別子Ｉdva を含む契約者レコードＲcsから、グループ識別子Ｉqpならびに全ての機器識別子Ｉdva およびＩdvb を取り出す（ステップＳ１３２）。次に、利用権管理部１１７は、受信設定要求Ｄrra から取り出した機器識別子Ｉdva、コンテンツ識別子Ｉcnt および利用条件Ｃcnt と、ユーザ情報ＤＢ１１３から得たグループ識別子Ｉqpならびに機器識別子Ｉdva およびＩdvb との組み合わせを、利用権レコードＲrqt として利用権ＤＢ１１４に登録する（ステップＳ１３３）。ここで、利用権管理部１１７は、設定要求Ｄrra 内の利用条件Ｃcnt で機器２１ａ が取得対象コンテンツデータＤcntを利用する権利の付与を要求しているとみなす。以上のことから、利用権管理部１１７は、設定要求Ｄrra から取り出した利用条件Ｃcnt を利用権情報Ｄrqt として扱う。つまり、利用権情報Ｄrqt は、利用条件Ｃcnt が示す条件下で、コンテンツデータＤcnt を機器２１ａ が利用する権利を示す。

【００３９】以上の登録処理により、利用権ＤＢ１１４は、図７（ｂ）に示すように、グループ識別子Ｉqp、機器識別子Ｉdva およびＩdvb、コンテンツ識別子Ｉcntならびに利用権情報Ｄrqt を含む利用権レコードＲrqtの集まりとなる。これによって、利用権管理部１１７は、契約者βの取得対象コンテンツデータＤcnt 毎に、その利用権を管理する。また、本実施形態の特徴の一つして、利用権レコードＲrqt に、ユーザ情報ＤＢ１１３から得た全ての機器識別子Ｉdva およびＩdvb を付加することで、機器２１ａ からの設定要求Ｄrra により、機器２１ａ および２１ｂ は、コンテンツデータＤcnt の利用権を共有できるようになる。利用権管理部１１７は、以上の利用条件登録処理が終了すると、今回受け取った設定要求Ｄrra をコンテンツ管理部１１８に渡す。

【００４０】今回の設定要求Ｄrra には、利用条件Ｃcnt として「再生ｍ回」（ｍは自然数）が設定されていると仮定すると、図７（ｂ）に示すように、今回新規登録される利用権レコードＲrqt は、「再生ｍ回」という条件が指定された利用権情報Ｄrqt を含むことになる。

【００４１】なお、本ライセンス情報管理システムＳａの技術的特徴とは関係ないが、ステップＳ１３において、利用権管理部１１７は、利用条件情報Ｄcrt の登録毎に、機器識別子Ｉdva が割り当てられている契約者βに、コンテンツデータＤcnt の利用に対する課金を行ってもよい。

【００４２】コンテンツ管理部１１８は、設定要求Ｄrraを受け取ると、コンテンツデータＤcnt およびそれ専用の暗号鍵Ｋe の読み出し処理を行う（ステップＳ１４）。より具体的には、コンテンツ管理部１１８は、受信設定要求Ｄrra から、コンテンツ識別子Ｉcnt を取り出す。その後、コンテンツ管理部１１８は、コンテンツＤＢ１１１にアクセスして、取り出したコンテンツ識別子Ｉcnt が割り当てられているコンテンツデータＤcntおよび暗号鍵Ｋe を読み出す。以上の読み出し処理が終了すると、コンテンツ管理部１１８は、読み出したコンテンツデータＤcnt および暗号鍵Ｋe をコンテンツ暗号化部１１９に渡す。さらに、コンテンツ管理部１１８は、受け取った設定要求Ｄrra を送信データ生成部１２０に渡す。

【００４３】コンテンツ暗号化部１１９は、コンテンツデータＤcnt の暗号処理を行う（ステップＳ１５）。より具体的には、コンテンツ暗号化部１１９は、受け取ったコンテンツデータＤcnt を、同時に受け取った暗号鍵Ｋe で暗号化して、前述の暗号済みコンテンツデータＤecntを生成する。コンテンツ暗号化部１１９は、以上の暗号処理が終了すると、暗号済みコンテンツデータＤecntを送信データ生成部１２０に渡す。

【００４４】送信データ生成部１２０は、コンテンツ管理部１１８からの設定要求Ｄrra と、コンテンツ暗号化部１１９からの暗号済みコンテンツデータＤecntとが揃うと、送信データ生成処理を行う（ステップＳ１６）。より具体的には、送信データ生成部１２０は、受信設定要求Ｄrra から、コンテンツ識別子Ｉcnt および機器識別子Ｉdva を取り出す。さらに、送信データ生成部１２０は、取り出した機器識別子Ｉdva およびコンテンツ識別子Ｉcnt を、受け取った暗号済みコンテンツデータＤecntに付加して、図９（ｂ）に示すような、送信データＤtrnaを生成する。送信データ生成部１２０は、以上の送信データ生成処理が終了すると、送信データＤtrnaを通信部１１５に渡す。通信部１１５は、受け取った送信データＤtrnaを、伝送路３１を介して、機器２１ａ へと

送信する（ステップＳ１７）。

【００４５】機器２１ａ（図４参照）において、通信部２１３は、伝送路３１を通じて送信されてくる送信データＤtmaを受信する（ステップＳ１８）。より具体的には、通信部２１３は、それに含まれる機器識別子Ｉdvaとコンテンツ識別子Ｉcnt とから、今回、取得対象コンテンツデータＤcnt を含む自分宛の送信データＤtmaを受信したことを認識する。このような認識結果に従って、通信部２１３は、受信データＤtmaをコンテンツ管理部２１４に渡す。

【００４６】コンテンツ管理部２１４は、受信データＤtma内のコンテンツ識別子Ｉcnt および暗号済みコンテンツデータＤecntを、コンテンツ蓄積部２１５に蓄積する（ステップＳ１９）。つまり、コンテンツ蓄積部２１５には、図１０に示すように、上述の設定要求Ｄrra を使って要求したコンテンツ識別子Ｉcnt および暗号済みコンテンツデータＤecntの組みが、いくつか蓄積されることになる。

【００４７】デジタルライツの保護の観点から、機器２１ａには暗号済みコンテンツデータＤecntが配信される。そのため、機器２１ａは、コンテンツデータＤcnt を利用する場合には、利用権管理装置１１により提供される復号鍵Ｋd で、暗号済みコンテンツデータＤecntを復号する必要がある。ここで、本ライセンス情報管理システムＳａでは、復号鍵Ｋd を機器２１ａに提供するために、ライセンス情報Ｄlca が用いられる。以下、図１１～図１３を参照して、ライセンス情報Ｄlca の取得およびコンテンツデータＤcnt の復号時における機器２１ａおよび利用権管理装置１１の動作について説明する。

【００４８】まず、ユーザβは、機器２１ａを操作して、コンテンツ蓄積部２１５に蓄積されている暗号済みコンテンツデータＤecntの中から、今回利用したいものを特定する。ここで、以下の説明において、今回指定された暗号済みコンテンツデータＤecntを、復号対象コンテンツデータＤecntと称する。ユーザβによる指定に応答して、機器２１ａは、図１４（ａ）に示すような発行要求Ｄira を生成し、利用権管理装置１１に送信する（図１１；ステップＳ２１）。発行要求Ｄira は、上述のライセンス情報Ｄlca の発行を利用権管理装置１１に機器２１ａが要求するための情報である。より具体的には、コンテンツ管理部２１４（図４参照）は、契約者βにより特定された復号対象コンテンツデータＤecntに付加されているコンテンツ識別子Ｉcnt を、コンテンツ蓄積部２１５から取り出して、発行要求生成部２１６に渡す。発行要求生成部２１６は、コンテンツ管理部２１４により取り出されたコンテンツ識別子Ｉcnt を受け取る。さらに、発行要求生成部２１６は、機器識別子格納部２１１から機器識別子Ｉdva を取り出す。その後、発行要求生成部２１６は、機器識別子Ｉdva およびコンテンツ識別子Ｉcnt の組み合わせに、発行要求識別子Ｉirを付加して、発行要求Ｄira （図１４（ａ）参照）を生成する。ここで、発行要求識別子Ｉirは、利用権管理装置１１が発行要求Ｄira を特定するために使用される。発行要求生成部２１６は、以上の発行要求Ｄira を通信部２１３に渡す。通信部２１３は、受け取った発行要求Ｄira を伝送路３１を通じて、利用権管理装置１１に送信する。

【００４９】利用権管理装置１１において、通信部１１５（図２参照）は、伝送路３１を通じて送信されてくる発行要求Ｄira を受信して、ユーザ認証部１１６に渡す。ユーザ認証部１１６は、発行要求Ｄira を受け取ると、ユーザ認証処理を行う（ステップＳ２２）。ステップＳ２２におけるユーザ認証は、ステップＳ１２のそれと同様であるため、詳細な説明を省略する。ユーザ認証部１１６は、ユーザ認証に成功した場合に限り、受信発行要求Ｄira を利用権管理部１１７に渡す。

【００５０】利用権管理部１１７は、それに設定されている発行要求識別子Ｉirを確認して、ユーザ認証部１１６から渡されたものが発行要求Ｄira であることを認識する。この認識結果に従って、利用権管理部１１７は、受け取った発行要求Ｄira から、機器識別子Ｉdva およびコンテンツ識別子Ｉcnt を取り出す（ステップＳ２３）。次に、利用権管理部１１７は、取り出した機器識別子Ｉdva およびコンテンツ識別子Ｉcnt の組み合わせと同じものを含む利用権レコードＲrqt が、利用権ＤＢ１１４（図７（ｂ）参照）に登録されているか否かを判断する（ステップＳ２４）。

【００５１】利用権管理部１１７は、ステップＳ２４で「Ｙｅｓ」と判断した場合、対象となる利用権レコードＲrqt に含まれる利用権情報Ｄrqt を参照して、機器２１ａに利用許可を与えることができるか否か、つまりコンテンツデータＤcnt の利用権が残っているか否かを判断する（ステップＳ２５）。ステップＳ２５で「Ｙｅｓ」と判断した場合、利用権管理部１１７は、対象となる利用権情報Ｄrqt を参照して、利用許可情報Ｄlwa を生成する（ステップＳ２６）。利用許可情報Ｄlwa は、復号対象コンテンツデータＤecntの復号許可を機器２１ａに与えるための情報である。また、利用許可情報Ｄlwa の生成により、機器２１ａの利用権情報Ｄrqt が使われることになるので、ステップＳ２６の次に、利用権管理部１１７は、ステップＳ２６で使われた分だけ利用権情報Ｄrqt を更新する（ステップＳ２７）。なお、ステップＳ２７の実行時点で、全ての利用権情報Ｄrqt が使われた場合には、それを含んでいた利用権レコードＲrqt を利用権ＤＢ１１４から削除しても良い。

【００５２】ここで、以上のステップＳ２５～Ｓ２７の処理の具体例について説明する。上述の仮定に従えば、今回対象となる利用権レコードＲrqt において、利用権情報Ｄrqt は、図７（ｂ）に示すように、「再生ｍ回」という利用権を表す。したがって、ステップＳ２５にお

いて、利用権管理部１１７は、機器２１ａに対し、復号対象コンテンツデータＤecntの再生許可を与えてもよいと判断する。この判断に従って、利用権管理部１１７は、ステップＳ２６で、利用許可情報Ｄlwa を作成する。この時生成される利用許可情報Ｄlwa としては、例えば、「再生ｎ回」が挙げられる。ここで、ｎは、上述のｍを超えない自然数であり、例えば、ユーザβが機器２１ａを操作して指定した値である。他にも、ｎは、機器２１ａの処理能力に応じて、利用権管理部１１７側で設定しても良い。また、ステップＳ２６により、機器２１ａが復号対象コンテンツデータＤecntを再生する権利をｎ回使うことになる。そのため、ステップＳ２７において、利用権管理部１１７は、利用権情報Ｄrqt を「再生ｍ回」から「再生（ｍ－ｎ）回」に更新する。

【００５３】以上の具体例では、利用権情報Ｄrqt がコンテンツデータＤcnt の再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムＳａでは、様々な利用権情報Ｄrqt （つまり利用条件Ｃcnt ）を設定することができる。従って、ステップＳ２３からＳ２７までの処理手順は、利用権情報Ｄrqt に応じて適切に規定される必要がある。

【００５４】以上の利用許可情報Ｄlwa を、利用権管理部１１７（図２参照）は、発行要求Ｄira と一緒に、ライセンス情報生成部１２１に渡す。より具体的には、ライセンス情報生成部１２１は、図３に示すように、ハッシュ値生成部１２１１およびライセンス情報組立部１２１２を含んでいる。ハッシュ値生成部１２１１には、利用許可情報Ｄlwa のみが渡され、また、ライセンス情報組立部１２１２には、利用許可情報Ｄlwa および発行要求Ｄira の双方が渡される。

【００５５】まず、ハッシュ値生成部１２１１は、予め保持するハッシュ関数ｆ（ｘ）に、受け取った利用許可情報Ｄlwa を代入して、利用許可情報Ｄlwa の改竄を防止するするためのハッシュ値Ｖhsa を生成する（ステップＳ２８）。つまり、ハッシュ値Ｖhsa は、利用許可情報Ｄlwa を生成多項式ｆ（ｘ）に代入した時に得られる解である。以上のようなハッシュ値Ｖhsa を、ハッシュ値生成部１２１１は、ライセンス情報組立部１２１２に渡す。

【００５６】ライセンス情報組立部１２１２は、受け取った発行要求Ｄira を復号鍵管理部１２２に渡す。復号鍵管理部１２２（図２参照）は、前述した復号鍵ＤＢ１１２（図６（ｂ）参照）を管理する。復号鍵管理部１２２は、受け取った発行要求Ｄira に設定されているコンテンツ識別子Ｉcnt および機器識別子Ｉdva を取り出す。さらに、復号鍵管理部１２２は、コンテンツ識別子Ｉcnt と同じ組みの復号鍵Ｋd を復号鍵ＤＢ１１２から取り出して、機器識別子Ｉdva と一緒に復号鍵暗号化部１２３に渡す。復号鍵暗号化部１２３は、受け取った復号鍵Ｋd を、同時に受け取った機器識別子Ｉdva を使って暗号化して（ステップＳ２９）、暗号済みの復号鍵Ｋeda を生成する。以上の暗号済み復号鍵Ｋeda および機器識別子Ｉdva は、ライセンス情報組立部１２１２に渡される。

【００５７】ライセンス情報組立部１２１２は、発行要求Ｄira および利用許可情報Ｄlwa、ハッシュ値Ｖhsa ならびに暗号済み復号鍵Ｋeda のすべてが揃うと、図１４（ｂ）に示すライセンス情報Ｄlca の生成を開始する（図１２：ステップＳ２１０）。より具体的には、ライセンス情報組立部１２１２は、発行要求Ｄira から、コンテンツ識別子Ｉcnt および機器識別子Ｉdva を取り出して、それぞれを、利用許可情報Ｄlwa 、暗号済み復号鍵Ｋeda およびハッシュ値Ｖhsa の組み合わせに付加する。さらに、ライセンス情報組立部１２１２は、予め保持するライセンス情報識別子Ｉlcを、機器識別子Ｉdva に付加して、ライセンス情報Ｄlca を生成する。以上のライセンス情報Ｄlca は、復号対象コンテンツデータＤecntの機器２１ａにおける利用を制御するための情報である。また、ライセンス情報識別子Ｉlcは、機器２１ａがライセンス情報Ｄlca を特定するための情報である。また、以上のライセンス情報Ｄlca は、通信部１１５および伝送路３１を通じて、機器２１ａに送信される（ステップＳ２１１）。

【００５８】機器２１ａ（図４参照）において、通信部２１３は、伝送路３１を通じて送信されてくるライセンス情報Ｄlca を受信する（ステップＳ２１２）。より具体的には、通信部２１３は、受信情報に含まれる機器識別子Ｉdva から、自分宛の情報が到着したと判断し、さらに、それに設定されるライセンス情報識別子Ｉlcから、今回、ライセンス情報Ｄlca を受け取ったことを認識する。このような認識結果に従って、通信部２１３は、受け取ったライセンス情報Ｄlca をライセンス情報処理部２１７に渡す。

【００５９】ライセンス情報処理部２１７は、図５に示すように、改竄判定部２１７１と、ハッシュ値生成部２１７２と、利用許可判定部２１７３と、復号鍵復号部２１７４とを含んでいる。通信部２１３からのライセンス情報Ｄlca は、まず、改竄判定部２１７１に渡される。改竄判定部２１７１は、まず、受け取ったライセンス情報Ｄlca から、利用許可情報Ｄlwa およびハッシュ値Ｖhsa を取り出し（ステップＳ２１３）、取り出した利用許可情報Ｄlwa を、ハッシュ値生成部２１７２に渡し、ハッシュ値Ｖhsa をそのまま保持する。ここで、以下の説明において混同が生じないように、ステップＳ２１３で取り出されたハッシュ値Ｖhsa を、機器２１ａの外部（つまり利用権管理装置１１）で生成されたものであるという観点から、外部ハッシュ値Vehsaと称する。

【００６０】ハッシュ値生成部２１７２は、利用権管理装置１１側のハッシュ値生成部１２１１（図３参照）と同じハッシュ関数ｆ（ｘ）を保持しており、受け取った

利用許可情報Ｄｌwa をハッシュ関数ｆ（ｘ）に代入してハッシュ値Ｖhsa を生成する（ステップＳ２１４）。ここでステップＳ２１４で生成されたハッシュ値Ｖhsaを、機器２１ａの内部で生成されたものであるという観点から、内部ハッシュ値Ｖｌhsaと称する。ハッシュ値生成部２１７２は、以上の内部ハッシュ値Ｖｌhsaを、改竄判定部２１７１に返す。

【００６１】改竄判定部２１７１は、上述の内部ハッシュ値Ｖｌhsaを受け取ると、利用許可情報Ｄｌwa が改竄されているか否かを判定する（ステップＳ２１５）。より具体的には、上述の内部ハッシュ値Ｖｌhsaは、ライセンス情報Ｄｌca 内の利用許可情報Ｄｌwa が改竄されていないという条件で、外部ハッシュ値Vehsaに一致する。そこで、ステップＳ２１５において、改竄判定部２１７１は、受け取った内部ハッシュ値Ｖｌhsaが外部ハッシュ値Vehsaに一致するか否かを判定する。改竄判定部２１７１は、「Ｙｅｓ」と判定した場合には、利用許可情報Ｄｌwa が改竄されておらず、今回送信されてきた利用許可情報Ｄｌwa が有効であるとみなして、今回受け取ったライセンス情報Ｄｌca を利用許可判定部２１７３に渡す。

【００６２】利用許可判定部２１７３は、受け取ったライセンス情報Ｄｌca を参照して、復号対象コンテンツデータＤecntの利用が許可されているか否かを判定する（ステップＳ２１６）。利用許可判定部２１７３は、ステップＳ２１６において「Ｙｅｓ」と判断した場合に限り、受け取ったライセンス情報Ｄｌca から、暗号済み復号鍵Ｋeda を取り出して、復号鍵復号部２１７４に渡す。

【００６３】ここで、以上のステップＳ２１６の処理の具体例について説明する。前述の仮定に従えば、今回のライセンス情報Ｄｌca の利用許可情報Ｄｌwa により、コンテンツデータＤcnt の再生がｎ回だけ許可されている。かかる場合、利用許可判定部２１７３は、ステップＳ２１６において、利用許可情報Ｄｌwa に設定される再生回数が１以上であれば、復号対象コンテンツデータＤecntの利用が許可されていると判断して、受け取ったライセンス情報Ｄｌca を復号鍵復号部２１７４に渡す。

【００６４】以上の具体例では、利用権情報Ｄrqt がコンテンツデータＤcnt の再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムＳａでは、様々な利用権情報Ｄrqt （つまり利用条件Ｃｎｔ）を設定することができる。従って、ステップＳ２１６の処理は、利用権情報Ｄrqt に応じて適切に規定される必要がある。

【００６５】復号鍵復号部２１７４は、利用許可判定部２１７３から暗号済み復号鍵Ｋedaを受け取る。さらに、復号鍵復号部２１７４は、機器識別子格納部２１１から機器識別子Ｉdva を取り出す。その後、復号鍵復号部２１７４は、暗号済み復号鍵Ｋeda を、機器識別子Ｉdva で復号して（ステップＳ２１７）、復号鍵Ｋｄをコンテンツ復号部２１８に渡す。

【００６６】ところで、コンテンツ管理部２１４は、以上のステップＳ２１７の次またはそれ以前に（図１２にはステップＳ２１７の直後の例が示されている）、今回の復号対象コンテンツデータＤecntをコンテンツ蓄積部２１５から取り出す（ステップＳ２１８）。取り出された復号対象コンテンツデータＤecntは、コンテンツ復号部２１８に渡される。コンテンツ復号部２１８は、復号鍵復号部２１７４から受け取った復号鍵Ｋｄで、復号対象コンテンツデータＤecntを復号して（ステップＳ２１９）、コンテンツデータＤcnt をコンテンツ再生部２１９に渡す。コンテンツ再生部２１９は、受け取ったコンテンツデータＤcnt を再生して、音声出力する（ステップＳ２２０）。これにより、契約者βは、事業者αから購入したコンテンツデータＤcnt が表す音楽を聴くことができる。

【００６７】ここで、図１２のステップＳ２１５を参照する。ステップＳ２１５において、改竄判定部２１７１は、利用許可情報Ｄｌwa が改竄されていると判定する場合がある。また、ステップＳ２１６において、利用許可判定部２１７３は、復号対象コンテンツデータＤecntの利用が許可されていないと判定する場合もある。このような場合、改竄判定部２１７１および利用許可判定部２１７３は、今回受け取ったライセンス情報Ｄｌca を破棄する（図１３；ステップＳ２２１）。以上から明らかなように、本ライセンス情報管理システムＳａでは、有効なライセンス情報Ｄｌca を受信した場合にのみ、復号対象コンテンツデータＤecntの復号が許可される。これによって、上述のデジタルライツが保護される。

【００６８】また、図１１のステップＳ２４において、利用権管理部１１７は、利用権レコードＲrqt が利用権ＤＢ１１４（図７（ｂ）参照）に登録されていないと判断する場合がある。さらに、ステップＳ２５において、利用権管理部１１７は、機器２１ａに利用許可を与えることができないと判断する場合もある。このような場合、利用権管理部１１７は、復号対象コンテンツデータＤecntの利用を拒否することを示す利用拒否情報Ｄrj（図１４（ｃ）参照）を生成して、通信部１１５に渡す。通信部１１５は、受け取った利用拒否情報Ｄrjを、伝送路３１を介して、機器２１ａに送信する（図１３：ステップＳ２２２）。

【００６９】機器２１ａ（図４参照）において、通信部２１３は、伝送路３１を通じて送信されてくる利用拒否情報Ｄrjを受信する（ステップＳ２２３）。利用拒否情報Ｄrjの受信以降、機器２１ａでは何の処理も行われない。以上から明らかなように、本ライセンス情報管理システムＳａでは、利用権ＤＢ１１４に有効な利用権レコードＲrqt が登録されてない場合には、利用拒否情報Ｄrjが、発行要求Ｄiraの送信元となる機器２１ａに送信される。これによって、機器２１ａ側では、復号対象コ

ンテンツデータＤecntは復号されない。これによって、上述のデジタルライツが保護される。

【００７０】なお、ステップＳ２４において、利用権管理部１１７は、利用権レコードＲrqt が利用権ＤＢ１１４（図７（ｂ）参照）に登録されていないと判断した後、利用権レコードＲrqt を新たに生成して、利用権ＤＢ１１４に登録するようにしてもよい。

【００７１】次に、以上の利用権レコードＲrqt の登録により、コンテンツデータＤcnt の利用権を機器２１ａと共有している機器２１ｂおよび利用権管理装置１１の間のデータ通信、およびそれに関連するそれぞれの動作について説明する。なお、以下の機器２１ｂの動作は、上述の機器２１ａの動作とほとんどの部分で同様であるから、その動作説明を簡素化する。まず、ユーザβは、機器２１ｂを操作して、コンテンツ識別子Ｉcnt および利用条件Ｃcnt を指定する。この指定に応答して、機器２１ｂは、設定要求Ｄrrb を生成し、利用権管理装置１１に送信する（図８；ステップＳ１１）。設定要求Ｄrrb は、設定要求Ｄrra と比較すると、機器識別子Ｉdva の代わりに、機器２１ｂを一意に特定する機器識別子Ｉdvb を含む点で相違するだけであるから、その詳細な説明を省略する。なお、機器２１ｂは、自身が利用可能な利用権レコードＲrqt が利用権ＤＢ１１４に登録されていることが予め分かっている場合には、利用条件Ｃcnt を含まない設定要求Ｄrrbを生成しても良い。

【００７２】利用権管理装置１１（図２参照）において、ユーザ認証部１１６は、通信部１１５を通じて、機器２１ｂからの設定要求Ｄrrb を受け取る。その後、ユーザ認証部１１６は、機器２１ｂが契約ユーザβの物であるか否かを判定するためのユーザ認証処理を行う（ステップＳ１２）。ユーザ認証部１１６は、ユーザ認証処理が成功した場合に限り、受け取った設定要求Ｄrrb を利用権管理部１１７に渡す。

【００７３】利用権管理部１１７は、今回の受信情報が設定要求Ｄrrb であることを認識すると、ステップＳ１３を行う。ステップＳ１３において、まず、利用権管理部１１７は、受信設定要求Ｄrrb 内の機器識別子Ｉdvb およびコンテンツ識別子Ｉcnt を含む利用権レコードＲrqt が利用権ＤＢ１１４（図７（ｂ）参照）に登録されているか否かを判断する（ステップＳ１３１）。前述したように、利用権ＤＢ１１４には、機器２１ａの設定要求Ｄrra に起因して、機器識別子Ｉdvb およびコンテンツ識別子Ｉcnt を含む利用権レコードＲrqt が登録済である。この場合、利用権管理部１１７は、ステップＳ１３２～Ｓ１３３を行うことなく、今回の設定要求Ｄrrb をコンテンツ管理部１１８に渡す。

【００７４】コンテンツ管理部１１８は、設定要求Ｄrrb の受信後、コンテンツデータＤcnt および暗号鍵Ｋeを読み出して（ステップＳ１４）、それらをコンテンツ暗号化部１１９に渡す。さらに、コンテンツ管理部１１８は、受信設定要求Ｄrrb を送信データ生成部１２０に渡す。コンテンツ暗号化部１１９は、コンテンツデータＤcnt の暗号処理を行い（ステップＳ１５）、それが終了すると、暗号済みコンテンツデータＤecntと受信設定要求Ｄrrb とを送信データ生成部１２０に渡す。

【００７５】送信データ生成部１２０は、前述したようにして、送信データＤtrnb（図９（ｂ）参照）を生成する（ステップＳ１６）。送信データＤtrnbは、送信データＤtrnaと比較すると、機器識別子Ｉdva の代わりに、機器識別子Ｉdvb を含む点で相違するだけであるから、その詳細な説明を省略する。ステップＳ１６の次に、送信データ生成部１２０は、送信データＤtrnbを通信部１１５に渡し、通信部１１５は、前述したように、受け取った送信データＤtrnbを機器２１ｂへと送信する（ステップＳ１７）。

【００７６】機器２１ｂ（図４参照）において、通信部２１３は、送信データＤtrnbを受信し（ステップＳ１８）、その後、受信データＤtrnbをコンテンツ管理部２１４に渡す。コンテンツ管理部２１４は、受信データＤtrnb内のコンテンツ識別子Ｉcnt および暗号済みコンテンツデータＤecntを、コンテンツ蓄積部２１５に蓄積する（ステップＳ１９）。

【００７７】デジタルライツの保護の観点から、機器２１ｂは、機器２１ａの場合と同様に、利用権管理装置１１からライセンス情報Ｄlcb の発行を受けなければ、コンテンツデータＤcnt を利用することができない。以下、図１１～図１３を参照して、ライセンス情報Ｄlcb の取得およびコンテンツデータＤcnt の復号時における機器２１ｂおよび利用権管理装置１１の動作について説明する。なお、この時の動作は、機器２１ａおよび利用権管理装置１１の動作とほとんどの部分で同様であるから、その動作説明を簡素化する。

【００７８】まず、ユーザβは、機器２１ｂを操作して、コンテンツ蓄積部２１５の中から、復号対象コンテンツデータＤecntを指定する。ユーザβの指定に応答して、機器２１ｂにおいて、発行要求生成部２１６は、発行要求Ｄirb（図１４（ａ）参照）を生成し、利用権管理装置１１に送信する（図１１；ステップＳ２１）。発行要求Ｄirb は、発行要求Ｄira と比較すると、機器識別子Ｉdva が機器識別子Ｉdvb に代わる点で相違するだけであるから、その詳細な説明を省略する。発行要求生成部２１６は、以上の発行要求Ｄirb を通信部２１３に渡す。通信部２１３は、受信発行要求Ｄirb を利用権管理装置１１に送信する。

【００７９】利用権管理装置１１において、ユーザ認証部１１６（図２参照）は、通信部１１５を通じて、機器２１ｂが送信した発行要求Ｄirb を受け取り、その後、ユーザ認証処理を行う（ステップＳ２２）。ユーザ認証部１１６は、ユーザ認証処理が成功した場合に限り、受信発行要求Ｄirb を利用権管理部１１７に渡す。利用権

管理部１１７は、受信発行要求Ｄirb から、機器識別子Ｉdvb およびコンテンツ識別子Ｉcnt を取り出し（ステップＳ２３）、その後、取り出した機器識別子Ｉdvb およびコンテンツ識別子Ｉcnt の組み合わせと同じものを含む利用権レコードＲrqt が、利用権ＤＢ１１４（図７（ｂ）参照）に登録されているか否かを判断する（ステップＳ２４）。

【００８０】利用権管理部１１７は、ステップＳ２４で「Ｙｅｓ」と判断した場合、対象となる利用権レコードＲrqt に含まれる利用権情報Ｄrqt を参照して、機器２１bに利用許可を与えることができるか否か、つまりコンテンツデータＤcnt の利用権が残っているか否かを判断する（ステップＳ２５）。ステップＳ２５で「Ｙｅｓ」と判断した場合、利用権管理部１１７は、対象となる利用権情報Ｄrqt を使って利用許可情報Ｄ１wb を生成する（ステップＳ２６）。利用許可情報Ｄ１wb は、利用許可情報Ｄ１wa と比較すると、機器識別子Ｉdva が機器識別子Ｉdvb に代わる点でのみ相違するから、その詳細な説明を省略する。ステップＳ２６の次に、利用権管理部１１７は、ステップＳ２６で使われた分だけ利用権情報Ｄrqt を更新する（ステップＳ２７）。

【００８１】以上の利用許可情報Ｄ１wb を、利用権管理部１１７（図２参照）は、発行要求Ｄirb と一緒に、ライセンス情報生成部１２１に渡す。ライセンス情報生成部１２１において、ハッシュ値生成部１２１１（図３参照）は、予め保持するハッシュ関数ｆ（ｘ）に、受け取った利用許可情報Ｄ１wb を代入して、利用許可情報Ｄ１wb の改竄を防止するするためのハッシュ値Ｖhsb を生成し（ステップＳ２８）、それをライセンス情報組立部１２１２に渡す。

【００８２】ライセンス情報組立部１２１２は、受け取った発行要求Ｄirb を復号鍵管理部１２２に渡す。復号鍵管理部１２２（図２参照）は、前述した復号鍵ＤＢ１１２（図６（ｂ）参照）を管理しており、受信発行要求Ｄirb からコンテンツ識別子Ｉcnt および機器識別子Ｉdvb を取り出す。さらに、復号鍵管理部１２２は、コンテンツ識別子Ｉcnt と同じ組みの復号鍵Ｋd を復号鍵ＤＢ１１２から取り出して、機器識別子Ｉdvb と一緒に復号鍵暗号化部１２３に渡す。復号鍵暗号化部１２３は、受け取った復号鍵Ｋd を、同時に受け取った機器識別子Ｉdvb を使って暗号化して（ステップＳ２９）、暗号済み復号鍵Ｋedb を生成する。以上の暗号済み復号鍵Ｋedb および機器識別子Ｉdvb は、ライセンス情報組立部１２１２に渡される。

【００８３】ライセンス情報組立部１２１２は、発行要求Ｄirb および利用許可情報Ｄ１wb、ハッシュ値Ｖhsb ならびに暗号済み復号鍵Ｋedb のすべてが揃うと、ライセンス情報Ｄ１cb（図１４（ｂ）参照）を生成する（図１２；ステップＳ２１０）。ライセンス情報Ｄ１cb は、ライセンス情報Ｄ１ca と比較すると、機器識別子Ｉdva、利用許可情報Ｄ１wa、暗号済み復号鍵Ｋeda およびハッシュ値Ｖhsa が機器識別子Ｉdvb、利用許可情報Ｄ１wb、暗号済み復号鍵Ｋedb およびハッシュ値Ｖhsb に代わる点で相違するだけであるから、その詳細な説明を省略する。以上のライセンス情報Ｄ１cb は、通信部１１５および伝送路３１を通じて、機器２１bに送信される（ステップＳ２１１）。

【００８４】機器２１ｂ（図４参照）において、通信部２１３は、伝送路３１を通じて送信されてくるライセンス情報Ｄ１cb を受信し（ステップＳ２１２）、それをライセンス情報処理部２１７に渡す。ライセンス情報処理部２１７において、改竄判定部２１７１は、受信ライセンス情報Ｄ１cb から、利用許可情報Ｄ１wb およびハッシュ値Ｖhsb を取り出し（ステップＳ２１３）、取り出した利用許可情報Ｄ１wbを、ハッシュ値生成部２１７２に渡し、ハッシュ値Ｖhsb を外部ハッシュ値Ｖehsbとして保持する。ハッシュ値生成部２１７２は、利用権管理装置１１側と同じハッシュ関数ｆ（ｘ）を保持しており、受け取った利用許可情報Ｄ１wb をハッシュ関数ｆ（ｘ）に代入して、内部ハッシュ値Ｖ１hsbを生成し（ステップＳ２１４）、それを改竄判定部２１７１に返す。

【００８５】改竄判定部２１７１は、前述と同様にして、上述の内部ハッシュ値Ｖ１hsbを受け取ると、それが外部ハッシュ値Ｖehsbに一致するか否かを判定し（ステップＳ２１５）、両者が一致する場合には、今回の利用許可情報Ｄ１wb が有効であるとして、受信ライセンス情報Ｄ１cb を利用許可判定部２１７３に渡す。利用許可判定部２１７３は、前述と同様にして、復号対象コンテンツデータＤecntの利用が許可されているか否かを判定し（ステップＳ２１６）、「Ｙｅｓ」と判断した場合に限り、受け取ったライセンス情報Ｄ１cb から、暗号済み復号鍵Ｋedb を取り出して、復号鍵復号部２１７４に渡す。復号鍵復号部２１７４は、利用許可判定部２１７３から暗号済み復号鍵Ｋedb を受け取る。さらに、復号鍵復号部２１７４は、機器識別子格納部２１１から機器識別子Ｉdvb を取り出す。その後、復号鍵復号部２１７４は、暗号済み復号鍵Ｋedb を、機器識別子Ｉdvb で復号して（ステップＳ２１７）、その結果得られる復号鍵Ｋd をコンテンツ復号部２１８に渡す。

【００８６】コンテンツ管理部２１４は、今回の復号対象コンテンツデータＤecntをコンテンツ蓄積部２１５から取り出し（ステップＳ２１８）、それをコンテンツ復号部２１８に渡す。コンテンツ復号部２１８は、復号鍵復号部２１７４からの復号鍵Ｋd で、復号対象コンテンツデータＤecntを復号して（ステップＳ２１９）、コンテンツデータＤcnt をコンテンツ再生部２１９に渡す。コンテンツ再生部２１９は、受け取ったコンテンツデータＤcnt を再生して、音声出力する（ステップＳ２２０）。

【００８７】以上のように本実施形態によれば、利用権

レコードＲrqt には、複数の機器識別子Ｉdva およびＩdvb が記録される。これによって、利用権管理装置１１は、互いに異なる機器２１ａおよび２１ｂから発行要求Ｄira およびＤirb が送信されてきたとしても、利用権レコードＲrqt を参照することで、同一の利用権情報Ｄrqt から生成されたライセンス情報Ｄ１ca およびＤ１cb をそれらに提供することができるようになる。以上の本実施形態によって、複数の機器が共通のデジタルライツを共有できる権利管理技術を提供することができる。

【００８８】なお、以上の実施形態では、利用権レコードＲrqt はグループ識別子Ｉgpを含んでいたが、これは、機器２１ａおよび２１ｂが同一グループに属することを明確にするためのものである。つまり、グループ識別子Ｉgpは、利用権レコードＲrqt に必須の情報ではない。また、利用権レコードＲrqt は、機器２１ａおよび２１ｂの機器識別子Ｉdva およびＩdvb を含まずに、グループ識別子Ｉgpのみを使って、同一グループに属する機器２１ａおよび２１ｂを特定するようにしても良い。

【００８９】また、以上の実施形態では、複数の機器２１の代表例として、２台の機器２１ａおよび機器２１ｂを挙げたが、これに限らず、３台以上の機器で、同一の利用権情報Ｄrqt を共有するようにしても良い。

【００９０】また、以上の実施形態では、図示の都合上、利用権管理装置１１がコンテンツＤＢ１１１を備えると説明したが、これに限らず、コンテンツデータＤcnt は別のサーバから機器２１ａおよび２１ｂに配信されても良い。

【００９１】また、以上の実施形態では、ユーザ情報ＤＢ１１３に契約時に登録された機器２１ａおよび２１ｂが同一の利用権情報Ｄrqt を共有する例について説明した。しかし、ユーザβ側の機器２１は、必ずしも機器２１ａおよび２１ｂの２台だけでコンテンツ配信を受けるわけではなく、新しく入手した機器２１を使ってコンテンツデータＤcnt を利用したい場合もある。以下に説明する利用権管理装置１１ａ～１１ｄは、上述の利用権管理装置１１の第１～第４の変型例であって、上述のニーズに対応するために提供される。「第１の変型例」

【００９２】図１５は、利用権管理装置１１ａを収容したライセンス情報管理システムＳａ１の全体構成を示すブロック図である。図１５のライセンス情報管理システムＳａ１は、図１のライセンス情報管理システムＳａと比較すると、利用権管理装置１１に代えて利用権管理装置１１ａを備えている点と、機器２１ｃをさらに備えている点で相違する。それ以外に両ライセンス情報管理システムＳａおよびＳａ１に相違点は無いので、図１５において、図１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。なお、図１５には、通信ケーブル３２が示されているが、これは第４の変型例で使われる構成であるため、本変型例だけでなく、第２および第３の変型例では、通信ケーブル３２の説明を省略する。

【００９３】利用権管理装置１１ａは、上述の事業者α側に設置され、図２の利用権管理装置１１と比較すると、図１６に示すように、ユーザ情報管理部１２４と、登録完了生成部１２５とをさらに備える点で相違する。それ以外に両利用権管理装置１１および１１ａの間に相違点は無い。それ故、図１６において、図２の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【００９４】機器２１ｃは、上述のユーザβにより所有されるが、現時点では、利用権管理装置１１ａのユーザ情報ＤＢ１１３に未登録の機器であって、図４の機器２１ａまたは２１ｂと比較すると、図１７に示すように、登録要求生成部２２０およびグループ識別子格納部２２１をさらに備える点で相違する。それ以外に、両機器２１ａおよび２１ｂと、機器２１ｃとの間には相違点は無い。それ故、図１７において、図４の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。なお、機器２１ｃの機器識別子格納部２１１には、機器２１ｃを一意に特定するための機器識別子Ｉdvc が予め格納されており、グループ情報格納部２２１には、ユーザβに割り当てられたグループ識別子Ｉgpが格納されていると仮定する。

【００９５】次に、図１８を参照して、以上のような構成のライセンス情報管理システムＳａ１において、機器２１ｃをユーザ情報ＤＢ１１３に登録するまでの機器２１ｃおよび利用権管理装置１１ａの動作について説明する。まず、機器２１ｃは、ユーザβの操作に従って、ユーザβが事業者αから通知されるグループ識別子Ｉgpを、グループ識別子格納部２２１に格納する。その後、ユーザβは、機器２１ｃを操作して、本機器２１ｃをユーザ情報ＤＢ１１３に登録する旨を指定する。この指定に応答して、機器２１ｃにおいて、登録要求生成部２２０は、図１９（ａ）に示す登録要求Ｄrsc を生成し、利用権管理装置１１ａに送信する（図１８；ステップＳ３１）。登録要求Ｄrsc は、本機器２１ｃをユーザ情報ＤＢ１１３に登録するよう利用権管理装置１１ａに要求するための情報である。ステップＳ３１をより具体的に説明すると、まず、登録要求生成部２２０は、機器識別子格納部２１１から機器識別子Ｉdvc を取り出し、さらに、グループ識別子格納部２２１からグループ識別子Ｉgpを取り出した後、取り出したグループ識別子Ｉgpおよび機器識別子Ｉdvc の組み合わせに、予め保持する登録要求識別子Ｉrsを付加して、登録要求Ｄrsc （図１９（ａ）参照）を生成する。ここで、登録要求識別子Ｉrsは、利用権管理装置１１ａが登録要求Ｄrsc を特定するために使用される。登録要求生成部２２０は、以上の登録要求Ｄrsc を通信部２１３に渡す。通信部２１３は、受け取った登録要求Ｄrsc を、伝送路３１を通じて、利用権管理装置１１ａに送信する。

【００９６】利用権管理装置１１ａ（図１６参照）において、通信部１１５は、伝送路３１を通じて送信されてくる情報を受信し、それに含まれる登録要求識別子Ｉrsから、今回の受信情報が登録要求Ｄrscであることを認識する。この認識結果に従って、通信部１１５は、受信登録要求Ｄrscを、ユーザ情報管理部１２４に渡す。ユーザ情報管理部１２４は、受信登録要求Ｄrscからグループ識別子Ｉqpを取り出した後、ユーザ情報ＤＢ１１３にアクセスして、取り出したグループ識別子Ｉqpを含む契約者レコードＲcs（図７（ａ）参照）を検索する（ステップＳ３２）。さらに、ユーザ情報管理部１２４は、検索した契約者レコードＲcsから機器識別子数Ｎdvを取り出す（ステップＳ３３）。

【００９７】次に、ユーザ情報管理部１２４は、取り出した機器識別子数Ｎdvが予め定められた上限値Ｖul以上であるか否かを判断する（ステップＳ３４）。ここで、上限値Ｖulは、ユーザβがユーザ情報ＤＢ１１３に登録可能な機器数の上限値である。ユーザ情報管理部１２４は、ステップＳ３４で、機器識別子数Ｎdvが上限値Ｖul以上でないと判断した場合には、受信登録要求Ｄrscから機器識別子Ｉdvcを取り出し、取り出したものを対象となる契約者レコードＲcsに追加する（ステップＳ３５）。さらに、ユーザ情報管理部１２４は、機器識別子数Ｎdvを１だけインクリメントする（ステップＳ３６）。その結果、契約者レコードＲcsは、図７（ａ）に示すものから、図２０に示すようなものに更新される。その後、ユーザ情報管理部１２４は、契約者レコードＲcsを正しく更新した旨を登録完了生成部１２５に通知し、さらに、受信登録要求Ｄrsc内の機器識別子Ｉdvcを登録完了生成部１２５に渡す。

【００９８】登録完了生成部１２５は、ユーザ情報管理部１２４から契約者レコードＤrscの更新が完了したことが通知されると、図１９（ｂ）に示す登録完了通知Ｄsccを生成し、機器２１ｃに送信する（ステップＳ３７）。登録完了通知Ｄsccは、本機器２１ｃをユーザ情報ＤＢ１１３に正しく登録したことを機器２１ｃに通知するための情報である。ステップＳ３７をより具体的に説明すると、まず、登録完了生成部１２５は、ユーザ情報管理部１２４から受け取った機器識別子Ｉdvcに、予め保持する登録完了識別子Ｉscを付加して、登録完了通知Ｄscc（図１９（ｂ）参照）を生成する。ここで、登録完了識別子Ｉscは、機器２１ｃが登録完了通知Ｄsccを特定するために使用される。登録完了生成部１２５は、以上の登録完了通知Ｄsccを通信部１１５に渡す。通信部１１５は、受け取った登録完了通知Ｄsccを、伝送路３１を通じて、機器２１ｃに送信する。

【００９９】機器２１ｃ（図１７参照）において、通信部２１３は、伝送路３１を通じて送信されてくる情報を受信し、それに含まれる登録完了識別子Ｉscから、今回の受信情報が登録完了通知Ｄsccであることを認識する。この認識結果に従って、通信部２１３は、受信登録完了通知Ｄsccを、設定要求生成部２１２に渡す。設定要求生成部２１２は、受信情報に設定されている登録完了識別子Ｉscから、今回登録完了通知Ｄsccを受信したことを認識する（ステップＳ３８）。この認識結果に従って、設定要求生成部２１２は図８のステップＳ１１を実行可能な状態になったと判断し、以降は第１の実施形態で説明した機器２１ａまたは機器２１ｂと同様に、利用権管理装置１１ａとデータ通信を行う。

【０１００】以上のように本変型例によれば、利用権管理装置１１ａおよび機器２１ｃのデータ通信により、ユーザβが新しい入手した機器２１ｃの機器識別子Ｉdvcを、ユーザ情報ＤＢ１１３に登録することが可能になるので、より使い勝手の良いライセンス情報管理システムＳａ1を提供できるようになる。

【０１０１】なお、ステップＳ３４において、機器識別子数Ｎdvが上限値Ｖul以上であると判断された場合、ユーザ情報管理部１２４は、ステップＳ３５～Ｓ３６のような処理を行わずに、契約者レコードＲcsの更新を拒否する旨を登録完了生成部１２５に通知し、さらに、受信登録要求Ｄrsc内の機器識別子Ｉdvcを登録完了生成部１２５に渡す。登録完了生成部１２５は、契約者レコードＤrscの更新拒否が通知されると、図１９（ｃ）に示す登録拒否通知Ｄsrcを生成し、通信部２１３および伝送路３１を通じて、機器２１ｃに送信する（ステップＳ３９）。登録拒否通知Ｄrscは、本機器２１ｃをユーザ情報ＤＢ１１３に登録できないことを機器２１ｃに通知するための情報であり、ユーザ情報管理部１２４から受け取った機器識別子Ｉdvcと、予め保持する登録拒否識別子Ｉsrを含む。機器２１ｃ（図１７参照）において、設定要求生成部２１２は、通信部２１３を通じて、登録拒否通知Ｄsrcを受け取り（ステップＳ３１０）、その通知に従って、設定要求生成部２１２は、図８のステップＳ１１を実行可能な状態ではないと判断し、処理を終了する。

【０１０２】また、ステップＳ３２において、ユーザ情報管理部１２４は、取り出したグループ識別子Ｉqpを含む契約者レコードＲcs（図７（ａ）参照）を見つけることができない場合には、ステップＳ３９と同様の処理を行って、機器識別子Ｉdvcのユーザ情報ＤＢ１１３への登録を拒否することが好ましい。

【０１０３】なお、以上の第１の変型例では、機器２１ｃおよび利用権管理装置１１ａがデータ通信を行うことにより、機器識別子Ｉdvcがユーザ情報ＤＢ１１３に登録されていた。しかし、これに限らず、以下の第２～第４の変型例のように、機器２１ｃと、他の機器２１ａまたは機器２１ｂとが協働して、機器識別子Ｉdvcがユーザ情報ＤＢ１１３に登録されるようにしても良い。

【０１０４】「第２の変型例」次に、第２の変型例に係る利用権管理装置１１ｂを収容したライセンス情報管理

31

システムＳａ2の全体構成について説明する。ライセンス情報管理システムＳａ2は、図１のライセンス情報管理システムＳａと比較すると、図１５に示すように、利用権管理装置１１に代えて利用権管理装置１１ｂを備えている点と、機器２１ｃをさらに備えている点で相違する。それ以外に両ライセンス情報管理システムＳａおよびＳａ2に相違点は無いので、図１５において、図１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【０１０５】利用権管理装置１１ｂは、上述の事業者α側に設置され、図２の利用権管理装置１１と比較すると、図２１に示すように、ユーザ情報管理部１２６と、登録完了生成部１２７とをさらに備える点で相違する。それ以外に両利用権管理装置１１および１１ｂの間に相違点は無い。それ故、図２１において、図２の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【０１０６】機器２１ａまたは機器２１ｂは、第１の実施形態で説明したように、ユーザβにより所有され、さらに、それぞれの機器識別子Ｉdva およびＩdvb は、利用権管理装置１１ｂのユーザ情報ＤＢ１１３に登録済みである（図７（ａ）参照）。また、機器２１ａまたは２１ｂは、機器２１ｃの機器識別子Ｉdvc の登録のために、図４と比較すると、図２２に示すように、機器識別子入力部２２２と、仮登録要求生成部２２３と、仮登録完了出力部２２４とをさらに備える点で相違する。それ以外に、本変型例に係る機器２１ａおよび２１ｂと、第１の実施形態に係るものとの間に相違点は無い。それ故、図２２において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１０７】機器２１ｃは、上述のユーザβにより所有されるが、現時点では、利用権管理装置１１ｂのユーザ情報ＤＢ１１３に未登録の機器であって、図４の機器２１aまたは２１ｂと比較すると、図２３に示すように、機器識別子入力部２２５および本登録要求生成部２２６をさらに備える点で相違する。それ以外に、両機器２１ａおよび２１ｂと、機器２１ｃとの間には相違点は無い。それ故、図２３において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１０８】次に、図２４および図２５を参照して、以上のような構成のライセンス情報管理システムＳａ2において、機器２１ｃの機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録するまでの機器２１ａ、機器２１ｃおよび利用権管理装置１１ｂの動作について説明する。ユーザβは、機器２１ａを操作して、機器識別子Ｉdvc をユーザ情報ＤＢ１１３に仮登録する旨を指定する。この指定に関連して、機器２１ａの機器識別子入力部２２２は、ユーザβが機器２１ａを操作することにより入力された機器２１ｃの機器識別子Ｉdvc を、仮登録要求生成部２２３に通知する（図２４：ステップＳ４１）。ここで、以下の説明では、機器２１ｃの機器識別子Ｉdvc を登録対象識別子Ｉdvc と称する。仮登録要求生成部２２３は、上述の通知に応答して、図２６（ａ）に示す仮登録要求Ｄprscを生成し、利用権管理装置１１ｂに送信する（ステップＳ４２）。仮登録要求Ｄprscは、登録対象識別子Ｉdvc をユーザ情報ＤＢ１１３に仮登録するよう利用権管理装置１１ｂに要求するための情報である。ステップＳ４２を具体的に説明すると、まず、仮登録要求生成部２２３は、機器識別子格納部２１１から機器識別子Ｉdva を取り出した後、取り出した機器識別子Ｉdva を登録済識別子Ｉdva として扱う。そして、仮登録要求生成部２２３は、登録済識別子Ｉdva および登録対象識別子Ｉdvc の組み合わせに、予め保持する仮登録要求識別子Ｉprs を付加して、仮登録要求Ｄprsc（図２６（ａ）参照）を生成する。ここで、仮登録要求識別子Ｉprs は、利用権管理装置１１ｂが仮登録要求Ｄprscを特定するために使用される。仮登録要求生成部２２３は、以上の仮登録要求Ｄprscを通信部２１３に渡す。通信部２１３は、受け取った仮登録要求Ｄprscを、伝送路３１を通じて、利用権管理装置１１bに送信する。

【０１０９】利用権管理装置１１ｂ（図２１参照）において、通信部１１５は、伝送路３１からの受信情報に仮登録要求識別子Ｉprs が含まれていることから、仮登録要求Ｄprscを今回受信したことを認識する。この認識結果に従って、通信部１１５は、受信仮登録要求Ｄprscを、ユーザ情報管理部１２６に渡す。ユーザ情報管理部１２６は、受信仮登録要求Ｄprscから登録済識別子Ｉdvaを取り出した後、ユーザ情報ＤＢ１１３にアクセスして、取り出した登録済識別子Ｉdva を含む契約者レコードＲcs（図７（ａ）参照）を検索する（ステップＳ４３）。その後、ユーザ情報管理部１２６は、図１８のステップＳ３３およびＳ３４と同様の処理を行って（ステップＳ４４，Ｓ４５）、ステップＳ４５において、機器識別子数Ｎdvが上限値Ｖul未満でないと判断した場合には、図１８のステップＳ３９と同様の処理を行う（ステップＳ４６）。この場合、機器２１ａは、図１８のステップＳ３１０と同様の処理を行う（ステップＳ４７）。

【０１１０】それに対して、ステップＳ４５において、機器識別子数Ｎdvが上限値Ｖul未満であると判断した場合に、受信仮登録要求Ｄprscから登録対象識別子Ｉdvc を取り出した後、取り出したものと、それが仮登録された機器識別子Ｉdvc であることを示す仮登録フラグＦps とを、対象となる契約者レコードＲcsに追加する（ステップＳ４８）。契約者レコードＲcsは、図７（ａ）に示すものから、図２７（ａ）に示すようなものに更新される。その後、ユーザ情報管理部１２６は、登録対象識別子Ｉdvc の仮登録が完了した旨を登録完了生成部１２７に通知し、さらに、受信仮登録要求Ｄprsc内の登録済識別子Ｉdva を登録完了生成部１２７に渡す。

32

【０１１１】登録完了生成部１２７は、ユーザ情報管理部１２６から仮登録が完了したことが通知されると、図２６（ｂ）に示す仮登録完了通知Ｄpsccを生成し、機器２１ａに送信する（ステップＳ４９）。仮登録完了通知Ｄpsccは、登録対象識別子Ｉdvc をユーザ情報ＤＢ１１３に仮登録したことを機器２１ａに通知するための情報である。ステップＳ４８をより具体的に説明すると、まず、登録完了生成部１２７は、ユーザ情報管理部１２６から受け取った登録済識別子Ｉdvaに、予め保持する仮登録完了識別子Ｉpsc を付加して、仮登録完了通知Ｄpscc（図２６（ｂ）参照）を生成する。ここで、仮登録完了識別子Ｉpsc は、機器２１ａが仮登録完了通知Ｄpsccを特定するために使用される。以上の仮登録完了通知Ｄpsccは、登録完了生成部１２７から、通信部１１５および伝送路３１を通じて、機器２１ａに送信される。

【０１１２】機器２１ａ（図２２参照）において、通信部２１３は、伝送路３１からの受信情報に含まれる仮登録完了識別子Ｉpsc および登録済識別子Ｉdva から、今回の受信情報が自分宛の仮登録完了通知Ｄpsccであることを認識する。この認識結果に従って、通信部２１３は、受信仮登録完了通知Ｄpsccを、仮登録完了出力部２２４に渡す。仮登録完了出力部２２４は、受信仮登録完了Ｄpsccに応答して、機器識別子Ｉdvc の仮登録が完了したことを、画像または音声で出力し（ステップＳ４１０）、そのことをユーザβに伝える。これによって、機器２１ａ側の処理が終了する。

【０１１３】仮登録完了を認識すると、ユーザβは、機器２１ｃを操作して、機器識別子Ｉdvc をユーザ情報ＤＢ１１３に本登録する旨を指定する。この指定に関連して、機器２１ｃの機器識別子入力部２２５は、ユーザβが機器２１ｃを操作することにより入力された機器２１ａの機器識別子（登録済識別子）Ｉdva を、本登録要求生成部２２６に通知する（図２５；ステップＳ５１）。この通知に応答して、本登録要求生成部２２６は、図２８（ａ）に示す本登録要求Ｄcrscを生成し、利用権管理装置１１ｂに送信する（ステップＳ５２）。本登録要求Ｄcrscは、機器識別子Ｉdvc をユーザ情報ＤＢ１１３に本登録するよう利用権管理装置１１ｂに要求するための情報である。ステップＳ５２を具体的に説明すると、まず、本登録要求生成部２２６は、機器識別子格納部２１１から機器識別子（つまり、登録対象識別子）Ｉdvc を取り出した後、取り出した登録対象識別子Ｉdvc と、通知された登録済識別子Ｉdva との組み合わせに、予め保持する本登録要求識別子Ｉcrs を付加して、本登録要求Ｄcrsc（図２８（ａ）参照）を生成する。ここで、本登録要求識別子Ｉcrs は、利用権管理装置１１ｂが本登録要求Ｄcrscを特定するために使用される。本登録要求生成部２２６は、以上の本登録要求Ｄcrscを、通信部２１３および伝送路３１を通じて、利用権管理装置１１ｂに送信する。

【０１１４】利用権管理装置１１ｂ（図２１参照）において、通信部１１５は、伝送路３１からの受信情報に含まれる本登録要求識別子Ｉcrs から、今回の受信情報が本登録要求Ｄcrscであることを認識する。この認識結果に従って、受信本登録要求Ｄcrscはユーザ情報管理部１２６に渡され、ユーザ情報管理部１２６は、受信本登録要求Ｄcrscから、機器識別子Ｉdva およびＩdvc の双方を取り出した後、ユーザ情報ＤＢ１１３にアクセスして、取り出した両機器識別子Ｉdva およびＩdvcを含む契約者レコードＲcs（図２７（ａ）参照）を検索する（ステップＳ５３）。その後、ユーザ情報管理部１２６は、検索した契約者レコードＲcsから、仮登録フラグＦpsを削除し（ステップＳ５４）、さらに、それに含まれる機器識別子数Ｎdvを１だけインクリメントする（ステップＳ５５）。これによって、機器識別子Ｉdvc の本登録が完了し、その結果、契約者レコードＲcsは、図２７（ａ）に示すものから、同図（ｂ）に示すようなものに更新される。その後、ユーザ情報管理部１２６は、登録対象識別子Ｉdvc の本登録が完了した旨を登録完了生成部１２７に通知し、さらに、受信本登録要求Ｄcrsd内の登録対象識別子Ｉdvc を登録完了生成部１２７に渡す。

【０１１５】登録完了生成部１２７は、ユーザ情報管理部１２６から本登録が完了したことが通知されると、図２８（ｂ）に示す本登録完了通知Ｄcsccを生成し、機器２１ｃに送信する（ステップＳ５６）。本登録完了通知Ｄcsccは、ユーザ情報ＤＢ１１３に機器識別子Ｉdvc の本登録が完了したことを機器２１ｃに通知するための情報である。ステップＳ５６をより具体的に説明すると、まず、登録完了生成部１２７は、ユーザ情報管理部１２６から受け取った登録対象識別子Ｉdvc を登録済識別子Ｉdvc として扱い、これに、予め保持する本登録完了識別子Ｉcsc を付加して、本登録完了通知Ｄcscc（図２８（ｂ）参照）を生成する。ここで、本登録完了識別子Ｉcsc は、機器２１ｃが本登録完了通知Ｄcsccを特定するために使用される。以上の本登録完了通知Ｄcsccは、通信部２１３および伝送路３１を通じて、機器２１ｃに送信される。

【０１１６】機器２１ｃ（図２３参照）において、通信部２１３は、伝送路３１を通じて送信されてくる情報を受信し、それに含まれる本登録完了識別子Ｉcsc および登録対象識別子Ｉdvc から、今回の受信情報が自分宛の本登録完了通知Ｄcsccであることを認識する。この認識結果に従って、通信部２１３は、受信本登録完了通知Ｄcsccを、設定要求生成部２１２に渡す。設定要求生成部２１２は、受信情報に設定されている本登録完了識別子Ｉcsc から、今回本登録完了通知Ｄcsccを受信したことを認識する（ステップＳ５７）。この認識結果に従って、設定要求生成部２１２は図８のステップＳ１１を実行可能な状態になったと判断し、以降は第１の実施形態で説明した機器２１ａまたは機器２１ｂと同様に、利用

権管理装置１１ｂとデータ通信を行う。

【０１１７】前述の第１の変型例に係る機器識別子Ｉｄｖｃの追加登録では、利用権管理装置１１ａは、機器２１ｃが本当にユーザβにより所有されているか否かを判断できないまま、機器識別子Ｉｄｖｃを、ユーザβの契約者レコードＲｃｓに登録していた。しかしながら、本変型例では、仮登録の時に機器２１ａが送信する仮登録要求Ｄｐｒｓｃに、登録済識別子Ｉｄｖａと、登録対象識別子Ｉｄｖｃとが設定され、本登録の時に機器２１ｃが送信する本登録要求Ｄｃｒｓｃに、登録済識別子Ｉｄｖａと、登録対象識別子Ｉｄｖｃとが設定されることにより、機器２１ａおよび２１ｃの間に関連性があることを証明することが可能となる。これによって、利用権管理装置１１ｂは、機器２１ｃが機器２１ａのユーザβにより所有されていると判断できる。このように、本変型例では、ユーザβの所有物でない機器２１がユーザβの契約者レコードＲｃｓに登録されにくい、機器識別子の追加登録を行えるライセンス情報管理システムＳａ2を提供できるようになる。

【０１１８】なお、以上の変型例では、機器２１ｃの機器識別子Ｉｄｖｃの追加登録のために、機器２１ａが動作する例について説明した。しかし、これに限らず、機器２１ｂも機器２１ａと同様に動作することで、機器識別子Ｉｄｖｃの追加登録に関与できるようになる。

【０１１９】「第３の変型例」次に、第３の変型例に係る利用権管理装置１１ｃを収容したライセンス情報管理システムＳａ3の全体構成について説明する。ライセンス情報管理システムＳａ3は、図１のライセンス情報管理システムＳａと比較すると、図１５に示すように、利用権管理装置１１に代えて利用権管理装置１１ｃを備えている点と、機器２１ｃをさらに備えている点で相違する。それ以外に両ライセンス情報管理システムＳａおよびＳａ3に相違点は無いので、図１５において、図１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【０１２０】利用権管理装置１１ｃは、上述の事業者α側に設置され、図２の利用権管理装置１１と比較すると、図２９に示すように、ユーザ情報管理部１２８と、パスワード通知生成部１２９と、登録完了生成部１３０とをさらに備える点で相違する。それ以外に両利用権管理装置１１および１１ｃの間に相違点は無い。それ故、図２９において、図２の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【０１２１】機器２１ａまたは機器２１ｂは、第１の実施形態で説明したように、ユーザβにより所有され、さらに、それぞれの機器識別子Ｉｄｖａおよび Ｉｄｖｂは、利用権管理装置１１ｃのユーザ情報ＤＢ１１３に登録済みである（図７（ａ）参照）。また、機器２１ａまたは２１ｂは、機器２１ｃの機器識別子Ｉｄｖｃの登録のために、図４と比較すると、図３０に示すように、パスワード入力部２２７と、登録要求生成部２２８と、登録完了出力部２２９とをさらに備える点で相違する。それ以外に、本変型例に係る機器２１ａおよび２１ｂと、第１の実施形態に係るものとの間に相違点は無い。それ故、図３０において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１２２】機器２１ｃは、上述のユーザβにより所有されるが、現時点では、利用権管理装置１１ｃのユーザ情報ＤＢ１１３に未登録の機器であって、図４の機器２１ａまたは２１ｂと比較すると、図３１に示すように、機器識別子入力部２３０、パスワード要求生成部２３１およびパスワード通知部２３２をさらに備える点で相違する。それ以外に、両機器２１ａおよび２１ｂと、機器２１ｃとの間には相違点は無い。それ故、図３１において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１２３】次に、図３２および図３３を参照して、以上のような構成のライセンス情報管理システムＳａ3において、機器２１ｃの機器識別子Ｉｄｖｃをユーザ情報ＤＢ１１３に登録するまでの機器２１ａ、機器２１ｃおよび利用権管理装置１１ｃの動作について説明する。ユーザβは、機器２１ｃを操作して、機器識別子Ｉｄｖｃをユーザ情報ＤＢ１１３に仮登録する旨を指定する。この指定に関連して、機器２１ｃの機器識別子入力部２３０は、ユーザβが機器２１ｃを操作することにより入力された機器２１ａの機器識別子（以下、登録済識別子と称する）Ｉｄｖａを、パスワード要求生成部２３１に通知する（図３２；ステップＳ６１）。パスワード要求生成部２３１は、上述の通知に応答して、図３４（ａ）に示すパスワード要求Ｄｒｐｓを生成し、利用権管理装置１１ｃに送信する（ステップＳ６２）。パスワード要求Ｄｒｐｓは、登録対象識別子Ｉｄｖｃをユーザ情報ＤＢ１１３に登録するために必要となるパスワードＷｐｓｓの発行を利用権管理装置１１ｃに要求するための情報である。ステップＳ６２を具体的に説明すると、まず、パスワード要求生成部２３１は、機器識別子格納部２１１から登録対象識別子Ｉｄｖｃを取り出した後、取り出した登録対象識別子Ｉｄｖｃと、通知された登録済識別子Ｉｄｖａとで構成される組みに、予め保持するパスワード要求識別子Ｉｒｐｓを付加して、パスワード要求Ｄｒｐｓ（図３４（ａ）参照）を生成する。ここで、パスワード要求識別子Ｉｒｐｓは、利用権管理装置１１ｃがパスワード要求Ｄｒｐｓを特定するために使用される。パスワード要求生成部２３１は、以上のパスワード要求Ｄｒｐｓを、通信部２１３および伝送路３１を通じて、利用権管理装置１１ｃの通信部１１５に送信する。

【０１２４】利用権管理装置１１ｃ（図２９参照）において、通信部１１５は、受信情報内のパスワード要求識別子Ｉｒｐｓから、パスワード要求Ｄｒｐｓを今回受信したことを認識する。この認識結果に従って、通信部１１５は、受信パスワード要求Ｄｒｐｓを、ユーザ情報管理部１

２８に渡す。ユーザ情報管理部１２８は、受信パスワード要求Ｄrps から登録済識別子Ｉdva を取り出した後、ユーザ情報ＤＢ１１３にアクセスして、取り出した登録済識別子Ｉdva を含む契約者レコードＲcs（図７（ａ）参照）を検索する（ステップＳ６３）。その後、ユーザ情報管理部１２８は、図１８のステップＳ３３およびＳ３４と同様の処理を行って（ステップＳ６４，Ｓ６５）、ステップＳ６５において、機器識別子数Ｎdvが上限値Ｖul以上であると判断した場合には、図１８のステップＳ３９と同様の処理を行う（ステップＳ６６）。この場合、機器２１ｃは、図１８のステップＳ３１０と同様の処理を行う（ステップＳ６７）。

【０１２５】それに対して、ステップＳ６５において、機器識別子数Ｎdvが上限値Ｖul以上でないと判断した場合に、ユーザ情報管理部１２８は、ステップＳ６８を行い、まず、上述のパスワードＷpss を生成する。パスワードＷpss は、典型的には、ユーザ情報管理部１２８が無作為に選んだ文字または記号の組み合わせであることが好ましい。さらに、ユーザ情報管理部１２８は、受信パスワード要求Ｄrpsから登録対象識別子Ｉdvc を取り出した後、取り出したものと、生成したパスワードＷpss とを、ステップＳ６３で検索した契約者レコードＲcs に追加して、登録対象識別子Ｉdvc の仮登録を行う（ステップＳ６８）。これによって、契約者レコードＲcs は、図７（ａ）に示すものから、図３５（ａ）に示すようなものに更新される。その後、ユーザ情報管理部１２８は、登録対象識別子Ｉdvc の仮登録が完了した旨をパスワード通知生成部１２９に通知し、さらに、受信パスワード要求Ｄrps 内の登録対象識別子Ｉdvc およびステップＳ６８で生成したパスワードＷpss を、パスワード通知生成部１２９に渡す。

【０１２６】パスワード通知生成部１２９は、ユーザ情報管理部１２８から仮登録が完了したことが通知されると、図３４（ｂ）に示すパスワード通知Ｄpss を生成し、機器２１ｃに送信する（ステップＳ６９）。パスワード通知Ｄpss は、登録対象識別子Ｉdvc の登録のために生成したパスワードＷpss を機器２１ｃに通知するための情報である。ステップＳ６９をより具体的に説明すると、まず、パスワード通知生成部１２９は、ユーザ情報管理部１２６から受け取った登録対象識別子Ｉdvc およびパスワードＷpss の組み合わせに、予め保持するパスワード通知識別子Ｉpss を付加して、パスワード通知Ｄpss（図３４（ｂ）参照）を生成する。ここで、パスワード通知識別子Ｉpss は、機器２１ｃがパスワード通知Ｄpss を特定するために使用される。以上のパスワード通知Ｄpss は、パスワード通知生成部１２９から、通信部１１５および伝送路３１を通じて、機器２１ｃの通信部２１３に送信される。

【０１２７】機器２１ｃ（図３１参照）において、通信部２１３は、受信信号内のパスワード通知識別子Ｉpss および登録対象識別子Ｉdvc から、今回の受信情報が自分宛のパスワード通知Ｄpss であることを認識する。この認識結果に従って、通信部２１３は、受信パスワード通知Ｄpss を、パスワード通知部２３２に渡す。パスワード通知部２３２は、パスワード通知Ｄpss に含まれるパスワードＷpss を画像出力または音声出力することで、それをユーザβに通知する（ステップＳ６１０）。これによって、機器２１ｃ側の処理が終了する。なお、ステップＳ６１０において、パスワード通知部２３２は、パスワードＷpss の通知に加えて、登録対象識別子Ｉdvc の仮登録が終了したことを画像または音声でユーザβに伝えても良い。

【０１２８】仮登録完了を認識すると、ユーザβは、機器２１ａを操作して、機器識別子Ｉdvc をユーザ情報ＤＢ１１３に本登録する旨を指定する。この指定に関連して、機器２１ａのパスワード入力部２２７は、ユーザβが機器２１ａを操作することにより入力されたパスワードＷpss を、登録要求生成部２２８に通知する（図３３；ステップＳ７１）。この通知に応答して、登録要求生成部２２８は、図３６（ａ）に示す登録要求Ｄrsc を生成し、利用権管理装置１１ｃに送信する（ステップＳ７２）。登録要求Ｄrsc は、登録対象識別子Ｉdvc をユーザ情報ＤＢ１１３に本登録するよう利用権管理装置１１ｃに要求するための情報である。ステップＳ７２を具体的に説明すると、まず、登録要求生成部２２８は、機器識別子格納部２１１から機器識別子（つまり、登録済識別子）Ｉdva を取り出した後、取り出したものと、通知されたパスワードＷpss との組みに、予め保持する登録要求識別子Ｉrsを付加して、登録要求Ｄrsc（図３６（ａ）参照）を生成する。ここで、登録要求識別子Ｉrs は、利用権管理装置１１ｃが登録要求Ｄrsc を特定するために使用される。登録要求生成部２２８は、以上の登録要求Ｄrsc を、通信部２１３および伝送路３１を通じて、利用権管理装置１１ｃに送信する。

【０１２９】利用権管理装置１１ｃ（図２９参照）において、通信部１１５は、受信情報に含まれる登録要求識別子Ｉrsから、今回の受信情報が登録要求Ｄrsc であることを認識する。この認識結果に従って、受信登録要求Ｄrsc はユーザ情報管理部１２８に渡され、ユーザ情報管理部１２８は、受信登録要求Ｄrsc から、登録済識別子Ｉdva およびパスワードＷpss の双方を取り出した後、ユーザ情報ＤＢ１１３にアクセスして、取り出した登録済識別子Ｉdva およびパスワードＷpss を含む契約者レコードＲcs（図３５（ａ）参照）を検索する（ステップＳ７３）。その後、ユーザ情報管理部１２８は、検索した契約者レコードＲcsから、パスワードＷpss を削除し（ステップＳ７４）、さらに、それに含まれる機器識別子数Ｎdvを１だけインクリメントする（ステップＳ７５）。これによって、機器識別子Ｉdvc の本登録が完了し、その結果、契約者レコードＲcsは、図３５（ａ）

に示すものから、同図（ｂ）に示すようなものに更新される。その後、ユーザ情報管理部１２８は、登録対象識別子Ｉdvc の本登録が完了した旨を登録完了生成部１３０に通知し、さらに、受信登録要求Ｄrsc 内の登録済識別子Ｉdva を登録完了生成部１３０に渡す。

【０１３０】登録完了生成部１３０は、ユーザ情報管理部１２８から本登録が完了したことが通知されると、図３６（ｂ）に示す登録完了通知Ｄscc を生成し、機器２１aに送信する（ステップＳ７６）。登録完了通知Ｄscc は、ユーザ情報ＤＢ１１３に機器識別子Ｉdvc の本登録が完了したことを機器２１ａに通知するための情報である。ステップＳ７６をより具体的に説明すると、まず、登録完了生成部１３０は、ユーザ情報管理部１２８から受け取った登録済識別子Ｉdva に、予め保持する登録完了識別子Ｉscを付加して、登録完了通知Ｄscc（図３６（ｂ）参照）を生成する。ここで、登録完了識別子Ｉscは、機器２１ａが本登録完了通知Ｄscc を特定するために使用される。以上の登録完了通知Ｄscc は、通信部１１５および伝送路３１を通じて、機器２１ａの通信部２１３に送信される。

【０１３１】機器２１ａ（図３０参照）において、通信部２１３は、受信情報に含まれる登録完了識別子Ｉscおよび登録済識別子Ｉdva から、今回の受信情報が自分宛の登録完了通知Ｄscc であることを認識する。この認識結果に従って、通信部２１３は、受信本登録完了通知Ｄscc を、登録完了出力部２２９に渡す。登録完了出力部２２９は、受信情報内の登録完了識別子Ｉscから、今回登録完了通知Ｄscc を受信したことを認識し、登録対象識別子Ｉdvc の本登録が完了したことを画像出力または音声出力して（ステップＳ７７）、ユーザβにその旨を伝える。これによって、機器２１ｃは、図８のステップＳ１１を実行可能な状態になる。そして、機器２１ｃは、必要に応じて、以降は第１の実施形態で説明した機器２１ａまたは機器２１ｂと同様の処理を行って、コンテンツデータＤcnt を利用する。

【０１３２】上述の第３の変型例によれば、利用権管理装置１１ｃのユーザ情報ＤＢ１１３に登録済みの機器２１ａが、未登録の機器２１ｃの機器識別子Ｉdvc の登録に関与することで、第２の変型例と同様に、ユーザβの所有物でない機器２１がユーザβの契約者レコードＲcs に登録されにくい、機器識別子の追加登録を行えるライセンス情報管理システムＳa3を提供できるようになる。

【０１３３】なお、以上の変型例では、機器２１ｃの機器識別子Ｉdvc の追加登録のために、機器２１ａが動作する例について説明した。しかし、これに限らず、機器２１ｂも機器２１ａと同様に動作することで、機器識別子Ｉdvc の追加登録に関与できるようになる。

【０１３４】「第４の変型例」次に、第４の変型例に係る利用権管理装置１１ｄを収容したライセンス情報管理システムＳa4の全体構成について説明する。ライセンス情報管理システムＳa4は、図１のライセンス情報管理システムＳａと比較すると、図１５に示すように、利用権管理装置１１に代えて利用権管理装置１１ｄを備えている点と、機器２１ｃをさらに備えている点と、機器２１ａおよび２１ｃが通信ケーブル３２を介して通信可能に接続される点とで相違する。それ以外に両ライセンス情報管理システムＳａおよびＳa4に相違点は無いので、図１５において、図１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【０１３５】利用権管理装置１１ｄは、上述の事業者α側に設置され、図２の利用権管理装置１１と比較すると、図３７に示すように、ユーザ情報管理部１３１と、登録完了生成部１３２とをさらに備える点で相違する。それ以外に両利用権管理装置１１および１１ｄの間に相違点は無い。それ故、図３７において、図２の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【０１３６】機器２１ａまたは２１ｂは、第１の実施形態で説明したように、ユーザβにより所有され、さらに、それぞれの機器識別子Ｉdva およびＩdvb は、利用権管理装置１１ｄのユーザ情報ＤＢ１１３に登録済みである（図７（ａ）参照）。また、機器２１ａまたは２１ｂは、機器２１ｃの機器識別子Ｉdvc の登録のために、図４と比較すると、図３８に示すように、通信部２２８と、登録要求生成部２２９と、登録完了通知部２３０とをさらに備える点で相違する。それ以外に、本変型例に係る機器２１ａおよび２１ｂと、第１の実施形態に係るものとの間に相違点は無い。それ故、図３８において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１３７】機器２１ｃは、上述のユーザβにより所有されるが、現時点では、自身に割り当てられた機器識別子Ｉdvc が利用権管理装置１１ｄのユーザ情報ＤＢ１１３に未登録であって、図４の機器２１ａまたは２１ｂと比較すると、図３９に示すように、登録要求生成部２３１と、通信部２３２とをさらに備える点で相違する。それ以外に、図４の両機器２１ａおよび２１ｂと、機器２１ｃとの間には相違点は無い。それ故、図３９において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１３８】次に、図４０を参照して、以上のような構成のライセンス情報管理システムＳa4において、機器２１ｃの機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録するまでの機器２１ａ、機器２１ｃおよび利用権管理装置１１ｄの動作について説明する。ユーザβは、機器２１ｃを操作して、機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録する旨を指定する。この指定に応答して、機器２１ｃの登録要求生成部２３１は、図４１（ａ）に示す第１の登録要求Ｄrsc1を生成し、通信ケーブル３２を通じて、機器２１ａに送信する（図４０：ステップＳ８

１）。第１の登録要求Ｄrsc1は、登録対象識別子Ｉdvcをユーザ情報ＤＢ１１３に登録することを、機器２１ｃの代わりに機器２１ａに要求するための情報である。ステップＳ８１を具体的に説明すると、まず、登録要求生成部２３１は、機器識別子格納部２１１から機器識別子（以下、登録対象識別子と称する）Ｉdvcを取り出した後、取り出した登録対象識別子Ｉdvcに、予め保持する第１の登録要求識別子Ｉrs1を付加して、第１の登録要求Ｄrsc1（図４１（ａ）参照）を生成する。ここで、第１の登録要求識別子Ｉrs1は、機器２１ａが第１の登録要求Ｄrsc1を特定するために使用される。登録要求生成部２３１は、以上の第１の登録要求Ｄrsc1を、通信部２３２および通信ケーブル３２を通じて、機器２１ａに送信する。

【０１３９】機器２１ａ（図３８参照）において、通信部２２８は、受信情報内の第１の登録要求識別子Ｉrs1から、第１の登録要求Ｄrsc1を今回受信したことを認識する（ステップＳ８２）。この認識結果に従って、通信部２２８は、受信した第１の登録要求Ｄrsc1を、登録要求生成部２２９に渡す。それに応答して、登録要求生成部２２９は、図４１（ｂ）に示す第２の登録要求Ｄrsc2を生成し、伝送路３１を通じて、利用権管理装置１１ｄに送信する（ステップＳ８３）。第２の登録要求Ｄrsc2は、登録対象識別子Ｉdvcをユーザ情報ＤＢ１１３に登録することを、利用権管理装置１１ｄに要求するための情報である。ステップＳ８３を具体的に説明すると、まず、登録要求生成部２２９は、機器識別子格納部２１１から機器識別子（以下、登録済識別子と称する）Ｉdvaを取り出した後、取り出した登録済識別子Ｉdvaを、今回受信した第１の登録要求Ｄrsc1に付加して、第２の登録要求Ｄrsc2（図４１（ｈ）参照）を生成する。ここで、第２の登録要求Ｄrsc2において、第１の登録要求識別子Ｉrs1は、利用権管理装置１１ｄが第２の登録要求Ｄrsc2を特定するために使用される。登録要求生成部２２９は、以上の第２の登録要求Ｄrsc2を、通信部２１３および伝送路３１を通じて、利用権管理装置１１ｄ（図３７参照）に送信する。

【０１４０】利用権管理装置１１ｄにおいて、通信部１１５は、伝送路３１からの受信情報内の第１の登録要求識別子Ｉrs1から、第２の登録要求Ｄrsc2を今回受信したことを認識する。その認識結果に従って、通信部１１５は、受信した第２の登録要求Ｄrsc2をユーザ情報管理部１３１に渡す。それに応答して、ユーザ情報管理部１３１は、受信した第２の登録要求Ｄrsc2から登録済識別子Ｉdvaを取り出し、ユーザ情報ＤＢ１１３にアクセスした後、図３２のステップＳ６３～Ｓ６５と同様の処理を行う（ステップＳ８４～Ｓ８６）。ユーザ情報管理部１３１は、ステップＳ８６において、機器識別子数Ｎdvが上限値Ｖul以上でないと判断した場合には、受信した第２の登録要求Ｄrsc2から登録対象識別子Ｉdvcを取り出した後、取り出したものを、ステップＳ８４で検索した契約者レコードＲcsに追加して、登録対象識別子Ｉdvcの登録を行う（ステップＳ８７）。これによって、契約者レコードＲcsは、図７（ａ）に示すものから、図３５（ａ）に示すようなものに更新される。その後、ユーザ情報管理部１３１は、登録対象識別子Ｉdvcの登録が完了した旨を登録完了生成部１３２に通知し、さらに、受信した第２の登録要求Ｄrsc2内の登録済識別子Ｉdvaを、登録完了生成部１３２に渡す。

【０１４１】登録完了生成部１３２は、ユーザ情報管理部１３１から登録完了が通知されると、図４１（ｃ）に示す登録完了通知Ｄsccを生成し、機器２１ａに送信する（ステップＳ８８）。登録完了通知Ｄsccは、登録対象識別子Ｉdvcのユーザ情報ＤＢ１１３への登録が完了したことを機器２１ａに通知するための情報である。ステップＳ８８をより具体的に説明すると、まず、登録完了生成部１３２は、ユーザ情報管理部１３１から受け取った登録済識別子Ｉdvaに、予め保持する登録完了識別子Ｉscを付加して、登録完了通知Ｄscc（図４１（ｃ）参照）を生成する。ここで、登録完了識別子Ｉscは、機器２１ａが登録完了通知Ｄsccを特定するために使用される。以上の登録完了通知Ｄsccは、登録完了生成部１３２から、通信部１１５および伝送路３１を通じて、機器２１ａの通信部２１３に送信される。

【０１４２】機器２１ａ（図３８参照）において、通信部２１３は、受信信号内の登録完了識別子Ｉscおよび登録済識別子Ｉdvaから、今回の受信情報が自分宛の登録完了通知Ｄsccであることを認識する。この認識結果に従って、通信部２１３は、受信登録完了通知Ｄsccを、登録完了通知部２３０に渡す。それに応じて、登録完了通知２３０は、登録対象識別子Ｉdvcの登録が完了したことを画像出力または音声出力することで、それをユーザβに通知する（ステップＳ６１０）。これによって、ユーザβは、機器２１ｃの機器識別子Ｉdvcが登録されたことを認識し、機器２１ｃは、図８のステップＳ１１を実行可能な状態になる。そして、機器２１ｃは、必要に応じて、以降は第１の実施形態で説明した機器２１ａまたは機器２１ｂと同様の処理を行って、コンテンツデータＤcntを利用する。

【０１４３】また、ステップＳ８６において、機器識別子数Ｎdvが上限値Ｖul以上であると判断された場合、従前の実施形態と同様に、利用権管理装置１１ｄから機器２１ａに、登録拒否通知Ｄrscが送信される（ステップＳ８１０，Ｓ８１１）。

【０１４４】上述の第４の変型例によれば、利用権管理装置１１ｄのユーザ情報ＤＢ１１３に登録済みの機器２１ａが、未登録の機器２１ｃの機器識別子Ｉdvcの登録に関与することで、第２の変型例と同様に、ユーザβの所有物でない機器２１がユーザβの契約者レコードＲcsに登録されにくい、機器識別子の追加登録を行えるライ

センス情報管理システムＳａ4を提供できるようになる。さらに、本変型例では、図３２および図３３の組み合わせと、図４０とを比較すれば分かるように、機器２１ａおよび２１ｃをケーブル３２で通信可能に接続することで、機器識別子Ｉdvc の登録までに必要な処理を減らすことができる。

【０１４５】なお、以上の変型例では、機器２１ｃの機器識別子Ｉdvc の追加登録のために、機器２１ａが動作する例について説明した。しかし、これに限らず、機器２１ｂも機器２１ａと同様に動作することで、機器識別子Ｉdvc の追加登録に関与できるようになる。

【０１４６】また、以上の変型例では、機器２１ａおよび機器２１ｃを通信可能に接続するために通信ケーブル３２を用いたが、これに限らず、機器２１ａおよび２１ｃは無線通信を行っても良い。他にも、機器２１ａおよび２１ｃは伝送路３１を介して通信を行っても良い。

【０１４７】また、以上の変型例では、登録完了通知Ｄscc は、利用権管理装置１１ｄから機器２１ａに送信されていた。しかし、これに限らず、利用権管理装置１１ｄから機器２１ｃに送信されても良い。また、機器２１ａに送信された登録完了通知Ｄscc は機器２１ｃに転送されても良い。この場合、登録完了したことは、機器２１ｃから音声または画像によりユーザβに通知される。

【０１４８】また、以上の第２～第４の変型例では、単一の機器２１ｃの機器識別子Ｉdvcをユーザ情報ＤＢ１１３に追加登録するための処理について説明したが、２台以上の機器２１の機器識別子Ｉdvを追加する場合にも、第２～第４の変型例を容易に応用することができる。

【０１４９】また、以上の第２～第４の変型例では、機器識別子Ｉdvc の追加登録に関与できるのは、機器２１ａでも、機器２１ｂでも良いと説明した。しかし、これに限らず、機器２１ａおよび２１ｂのいずれか一方に、機器識別子Ｉdvの追加登録に関与できる権限を与え、権限を持つ機器２１のみが機器識別子Ｉdvの追加登録に関与できるようにしても良い。

【０１５０】また、以上の第１～第４の変型例において、ユーザ情報ＤＢ１１３には、図７（ａ）に示す情報の他に、ユーザβに関連するユーザ情報をさらに登録しておき、機器２１ａまたは２１ｃは、利用権管理装置１１ａ～１１ｄにアクセスする際に、ユーザβにより入力されたユーザ情報を送信する。利用権管理装置１１ａ～１１ｄは、受信ユーザ情報を、予め格納されているユーザ情報と照合することで、機器２１ｃが機器２１ａと同じユーザβにより所有されているか否かを判断するようにしても良い。

【０１５１】また、第１の実施形態では、ユーザ情報ＤＢ１１３に契約時に登録された機器２１ａおよび２１ｂが同一の利用権情報Ｄrqt を共有する例について説明した。しかし、ユーザβは、ユーザ情報ＤＢ１１３または利用権ＤＢ１１４から、既に登録されている機器２１ｂの機器識別子Ｉdvb を削除したい場合がある。以下に説明する利用権管理装置１１ｅは、上述の利用権管理装置１１の第５の変型例であって、上述のニーズに対応するために提供される。

【０１５２】「第５の変型例」図４２は、利用権管理装置１１ｅを収容したライセンス情報管理システムＳa5の全体構成を示すブロック図である。ライセンス情報管理システムＳa5は、図１のライセンス情報管理システムＳａと比較すると、利用権管理装置１１が利用権管理装置１１ｅに代わる点でのみ相違する。それ以外に両ライセンス情報管理システムＳａおよびＳa5に相違点は無い。それ故、図４２において、図１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略する。

【０１５３】利用権管理装置１１ｅは、上述の事業者α側に設置され、図２の利用権管理装置１１と比較すると、図４３に示すように、機器識別子削除部１３３および削除完了作成部１３４をさらに備える点で相違する。それ以外に両利用権管理装置１１および１１ｅの間に相違点は無い。それ故、図４３において、図２の構成に相当するものの内、本変型例に関連の無い構成の図示および説明を省略する。

【０１５４】機器２１ａまたは２１ｂは、第１の実施形態で説明したように、ユーザβにより所有され、さらに、それぞれの機器識別子Ｉdva およびＩdvb は、利用権管理装置１１ｅのユーザ情報ＤＢ１１３に登録済みである（図７（ａ）参照）。さらに、機器２１ａおよび２１ｂは、利用権管理装置１１ｅの利用権ＤＢ１１４に登録されている利用権レコードＲrqt を共有している（図７（ｂ）参照）。また、機器２１ｂは、機器識別子Ｉdvb の削除のために、図４と比較すると、図４４に示すように、削除要求生成部２３３と、削除完了通知部２３４とをさらに備える点で相違する。それ以外に、本変型例に係る機器２１ｂと、第１の実施形態に係るものとの間に相違点は無い。それ故、図４４において、図４の構成に相当するものの内、本変型例に無関係な構成の図示および説明を省略する。

【０１５５】次に、図４５を参照して、以上のような構成のライセンス情報管理システムＳa5において、機器２１ｂの機器識別子Ｉdvb をユーザ情報ＤＢ１１３および利用権ＤＢ１１４から削除するまでの機器２１ｂおよび利用権管理装置１１ｅの動作について説明する。ユーザβは、機器２１ｂを操作して、機器識別子Ｉdvb をユーザ情報ＤＢ１１３および利用権ＤＢ１１４から削除する旨を指定する。この指定に応答して、機器２１ｂにおいて、削除要求生成部２３３は、図４６（ａ）に示す削除要求Ｄrvb を生成し、利用権管理装置１１ｅに送信する（図４５；ステップＳ９１）。削除要求Ｄrvb は、本機器２１ｂをユーザ情報ＤＢ１１３および利用権ＤＢ１１４から削除するよう利用権管理装置１１ｅに要求するた

めの情報である。ステップＳ９１をより具体的に説明すると、まず、削除要求生成部２３３は、機器識別子格納部２１１から機器識別子Ｉdvb を取り出した後、取り出したものを削除対象識別子Ｉdvb として、予め保持する削除要求識別子Ｉrwを付加して、削除要求Ｄrwb （図４６（ａ）参照）を生成する。ここで、削除要求識別子Ｉrwは、利用権管理装置１１ｅが削除要求Ｄrwb を特定するために使用される。以上の削除要求Ｄrwb は、削除要求生成部２３３から、通信部２１３および伝送路３１を通じて、利用権管理装置１１ｅに送信される。

【０１５６】利用権管理装置１１ｅ（図４３参照）において、通信部１１５は、伝送路３１からの受信情報に含まれる削除要求識別子Ｉrwから、今回の受信情報が削除要求Ｄrwb であることを認識する。この認識結果に従って、通信部１１５は、受信削除要求Ｄrwb を、機器識別子削除部１３３に渡す。機器識別子削除部１３３は、受信削除要求Ｄrwb から削除対象識別子Ｉdvb を取り出した後、ユーザ情報ＤＢ１１３内の契約者レコードＲcs（図７（ａ）参照）から、取り出した削除対象識別子Ｉdvb を検索して削除する（ステップＳ９２）。さらに、機器識別子削除部１３３は、ステップＳ９２で検索した契約者レコードＲcsに含まれる機器識別子数Ｎdvを１だけデクリメントする（ステップＳ９３）。その結果、契約者レコードＲcsは、図７（ａ）に示すものから、図４７（ａ）に示すようなものに更新される。

【０１５７】さらに、機器識別子削除部１３３は、利用権ＤＢ１１４内の利用権レコードＲrqt から、受信削除要求Ｉrwb から取り出した削除対象識別子Ｉdvb を検索して削除する（ステップＳ９４）。その結果、利用権レコードＲrqt は、図７（ｂ）に示すものから、図４７（ｂ）に示すようなものに更新される。その後、機器識別子削除部１３３は、契約者レコードＲcsおよび利用権レコードＲrqt を正しく更新した旨と、受信登録要求Ｄrsc 内の削除対象識別子Ｉdvb とを削除完了生成部１３４に通知する。

【０１５８】削除完了生成部１３４は、削除対象識別子Ｉdvb の削除が完了したことが通知されると、図４６（ｂ）に示す削除完了通知Ｄswb を生成し、機器２１ｂに送信する（ステップＳ９５）。削除完了通知Ｄswb は、削除対象識別子Ｉdvb を削除したことを機器２１ｂに通知するための情報である。ステップＳ９５をより具体的に説明すると、まず、削除完了生成部１３４は、受け取った削除対象識別子Ｉdvb に、予め保持する削除完了識別子Ｉswを付加して、削除完了通知Ｄswb （図４６（ｂ）参照）を生成する。ここで、削除完了識別子Ｉswは、機器２１ｂが削除完了通知Ｄswb を特定するために使用される。以上の削除完了通知Ｄswb は、通信部１１５および伝送路３１を通じて、機器２１ｂに送信される。

【０１５９】機器２１ｂ（図４３参照）において、通信部２１３は、伝送路３１からの受信情報に含まれる削除完了識別子Ｉswから、今回の受信情報が削除完了通知Ｄswbであることを認識する。この認識結果に従って、通信部２１３は、受信削除完了通知Ｄswb を、削除完了通知部２３４に渡す。削除完了通知部２３４は、削除完了通知Ｄswb を受信し（ステップＳ９６）、その後、機器識別子Ｉdvb が正常に削除されたことを、画像または音声で出力して、ユーザβにその旨を通知する。

【０１６０】以上のように本変型例によれば、利用権管理装置１１ｅおよび機器２１ｂのデータ通信により、ユーザβが不必要となった機器２１ｂの機器識別子Ｉdvb を、ユーザ情報ＤＢ１１３および利用権ＤＢ１１４から削除することが可能になるので、より使い勝手の良いライセンス情報管理システムＳa5を提供できるようになる。

【０１６１】なお、以上の変型例では、機器２１ｂ自身が、機器識別子Ｉdvb の削除要求Ｄrwb を生成して利用権管理装置１１ｅに送信するようにしたが、これに限らず、機器２１ａが、機器２１ｂの代わりに、削除要求Ｄrwb を生成して、利用権管理装置１１ｅに送信するようにしても良い。さらに、機器２１ａおよび２１ｂのいずれかに削除要求Ｄrwb を生成する権限を与え、権限が与えられた機器２１ａまたは２１ｂのみが削除要求Ｄrwb を利用権管理装置１１ｅに送信可能にしても良い。

【０１６２】また、以上の変型例では、削除要求Ｄrwb には、１個の削除対象識別子Ｉdvbが設定されるように説明したが、これに限らず、複数の機器識別子Ｉdvが設定されても良い。さらに、削除要求Ｄrwb が、第１の実施形態で説明したグループ識別子Ｉgpを含んでいる場合には、利用権管理装置１１ｅは、ユーザ情報ＤＢ１１３から、そのグループ識別子Ｉgpを含む契約者レコードＲcsを削除し、さらに、利用権ＤＢ１１４から、そのグループ識別子Ｉgpを含む利用権レコードＲrqt の全てを削除するようにしても良い。

【０１６３】「第２の実施形態」図４８は、本発明の第２の実施形態に係る利用権管理装置４１を収容したライセンス情報管理システムＳｂの全体構成を示すブロック図である。図４８において、ライセンス情報管理システムＳｂは、利用権管理装置４１の他に、複数の機器５１の一例として２つの機器５１ａおよび５１ｂと、伝送路６１とを備えている。利用権管理装置４１は、コンテンツ配信に関わる事業者α側に設置される。また、機器５１ａおよび５１ｂは、典型的には、事業者αとの契約に基づいてコンテンツ配信を受ける契約者βにより使用される。また、伝送路６１は、有線または無線であり、利用権管理装置４１と、機器５１ａまたは機器５１ｂとをデータ通信可能に接続する。

【０１６４】次に、図４９を参照して、図４８の利用権管理装置４１の詳細な構成について説明する。図４９の利用権管理装置４１は、図２の利用権管理装置１１と比

較すると、利用権データベース１１４および利用権管理部１１７の代わりに、利用権データベース（以下、利用権ＤＢと称す）４１１および利用権管理部４１２を備えている点で相違する。それ以外に、両利用権管理装置１１および４１の間に構成面での相違点は無い。それ故、図４９において、図２の利用権管理装置１１の構成に相当するものには同一の参照符号を付け、それぞれの説明を省略すると共に、本実施形態で説明が不要となる構成の図示を省略する。

【０１６５】次に、図５０を参照して、図４８の機器５１ａおよび５１ｂの詳細な構成について説明する。図５０の機器５１ａおよび５１ｂは、図４の機器２１ａおよび２１ｂと比較して、設定要求生成部２１２の代わりに、設定要求生成部５１１を備えている点で相違する。それ以外に、機器５１ａおよび５１ｂと、機器２１ａおよび２１ｂとの間に構成面での相違点は無い。それ故、図５０において、図４の機器２１ａまたは２１ｂの構成に相当するものには同一の参照符号を付け、それぞれの説明を省略すると共に、本実施形態で説明が不要となる構成の図示を省略する。

【０１６６】次に、上記ライセンス情報管理システムＳｂにおいても、前述のライセンス情報管理システムＳａの場合と同様に、契約者βは事業者αからコンテンツ配信を受けるために必要となる準備を行う。この準備作業において、図６（ａ）、図６（ｂ）および図７（ａ）に示すコンテンツＤＢ１１１、復号鍵ＤＢ１１２およびユーザ情報ＤＢ１１３とが構築される。これらの詳細については、第１の実施形態で既に詳説しているので、本実施形態ではそれぞれの説明を省略する。

【０１６７】また、以上の準備作業において、事業者αは、機器５１ａおよび５１ｂに、それらを一意に特定するための機器識別子Ｉdva およびＩdvb を割り当てる場合がある。以上の機器識別子Ｉdva は、図５０に示す機器５１ａの機器識別子格納部２１１に設定され、機器識別子Ｉdvb は、機器５１ｂの機器識別子格納部２１１に設定される。なお、機器識別子Ｉdva およびＩdvb は、工場出荷時にそれぞれの機器識別子格納部２１１に設定されていても良い。

【０１６８】以上の準備が終了すると、機器５１ａおよび５１ｂの一方は、ユーザβの操作に従って、利用権管理装置４１から、コンテンツデータＤcnt を取得することが可能となる。以下、図５１のフローチャートを参照して、コンテンツデータＤcnt の取得時における機器５１ａおよび利用権管理装置４１の間のデータ通信、およびそれに関連するそれぞれの動作について説明する。なお、コンテンツデータＤcnt の取得時における機器５１ｂおよび利用権管理装置４１の間のデータ通信、およびそれに関連するそれぞれの動作については、機器５１ａのものと同様であるため、それぞれの説明を省略する。ここで、図５１は、図８と比較すると、ステップＳ１０１およびＳ１０３をさらに含む点と、ステップＳ１３の代わりにステップＳ１０２を含む点とで相違する。それ以外に両フローチャートに相違点は無いので、図５１において、図８のステップに相当するものには同一のステップ番号を付け、それぞれの説明を省略する。

【０１６９】ユーザβは、機器５１ａを操作して、利用権管理装置４１にアクセスし、コンテンツＤＢ１１１内のコンテンツデータＤcnt から、今回取得したいもののコンテンツ識別子Ｉcnt を指定する。以降の説明において、今回指定されたコンテンツデータＤcnt を、取得対象コンテンツデータＤcnt と称する。さらに、ユーザβは、取得対象コンテンツデータＤcnt を利用する際の利用条件Ｃcnt （第１の実施形態参照）を指定する。

【０１７０】この指定に応答して、機器５１ａの設定要求生成部５１１は、今回指定されたものの中に共有対象識別子Ｉdvが含まれているか否かを判断する（ステップＳ１０１）。ここで、共有対象識別子Ｉdvとは、本ステップＳ１０１を実行する機器５１以外の他の機器５１の機器識別子Ｉdvであって、共有対象となる利用権レコードＲrotaに登録済の機器５１の機器識別子Ｉdvである。上述から明らかなように、今回指定されるものには、共有対象識別子Ｉdvは含まれないので、設定要求生成部５１１は、図９（ａ）の同様の形式を有する第１の設定要求Ｄrra （第１の実施形態参照）を生成し、伝送路６１を通じて、利用権管理装置４１に送信する（ステップＳ１１）。本実施形態において、第１の設定要求Ｄrra に含まれる設定要求識別子Ｉrrは、利用権管理装置４１が受信情報が第１の設定要求Ｄrraおよび第２の設定要求Ｄrr2b のいずれかであることを特定するために使用される。

【０１７１】利用権管理装置４１（図４９参照）において、ユーザ認証部１１６は、伝送路６１からの第１の設定要求Ｄrra の受信に応答して、認証処理を行い（ステップＳ１２）、その後、受け取った第１の設定要求Ｄrra を利用権管理部４１２に渡す。利用権管理部４１２は、ユーザ認証部１１６からの受信情報内の設定要求識別子Ｉrrに基づいて、今回の受信情報が第１の設定要求Ｄrra または第２の設定要求Ｄrr2bのいずれかであることを認識する。この認識結果に従って、利用権管理部４１２は、利用権データベース（以下、利用権ＤＢと称する）１１４への利用権登録処理を行う（ステップＳ１０２）。ステップＳ１０２において、より具体的には、利用権管理部４１２は、今回、第１の設定要求Ｄrra を受信したか否かを判断する（ステップＳ１０２１）。ここで、ステップＳ１０２１では、受信情報が共有対象識別子Ｉdvb を含んでいる場合には、第１の設定要求Ｄrra を受信したと、利用権管理部４１２は判断する。それに対して、共有対象識別子Ｉdvb を含んでいない場合には、後述する第２の設定要求Ｄrr2bを受信したと、利用権管理部４１２は判断する。今回の場合、利用権管理部

４１２は、第１の設定要求Ｄrra を受信したと判断することになるから、ステップＳ１０２２を行う。

【０１７２】ステップＳ１０２２において、利用権管理部４１２は、受信した第１の設定要求Ｄrra から、機器識別子Ｉdva 、コンテンツ識別子Ｉcnt および利用条件Ｃcnt を取り出す。さらに、利用権管理部４１２は、利用権ＤＢ４１１にアクセスして、取り出したものを利用権レコードＲrqtaとして登録する（ステップＳ１０２２）。ここで、第１の実施形態と同様に、利用条件Ｃcntは、利用権情報Ｄrqtとして使われる。以上のステップＳ１０２２により、利用権ＤＢ１１４は、図５２（ａ）に示すように、機器識別子Ｉdva および／または機器識別子Ｉdvb、コンテンツ識別子Ｉcnt ならびに利用権情報Ｄrqt を含む利用権レコードＲrqtaの集まりとなる。ところで、第１の実施形態では、図８のステップＳ１３２およびＳ１３３で説明したように、利用権管理部１１７は、機器２１ａの設定要求Ｄrra の受信に応答して、ユーザ情報ＤＢ１１３から同一グループに属する全機器識別子Ｉdva および Ｉdvb を取り出し、それらを全て利用権レコードＲrqt に登録していた。それに対して、第２の実施形態では、利用権管理部４１２は、ステップＳ１０２２の時点では、第１の設定要求Ｄrra の送信元となる機器識別子Ｉdvaのみを利用権レコードＲrqt に登録する。この点で、第１および第２の実施形態は顕著に相違する。

【０１７３】以上のステップＳ１０２２が終了すると、今回受け取った第１の設定要求Ｄrra を、利用権管理部４１２はコンテンツ管理部１１８に渡す。以降、利用権管理装置４１は、利用権管理装置１１と同様に、ステップＳ１４～Ｓ１７を実行し、その後、機器５１ａは、機器２１ａと同様に、ステップＳ１８～Ｓ１９を実行する。その結果、機器５１ａは、利用権管理装置４１から、図９（ｂ）に示す形式を有する送信データＤtmaを受信する。また、本ライセンス情報管理システムＳb においても、機器５１ａは、暗号済コンテンツデータＤecntを復号するために、ライセンス情報Ｄlca （第１の実施形態参照）を利用権管理装置４１から受け取るが、この時の動作については第１の実施形態と同様であるため（図１１、図１２参照）、その説明を省略する。

【０１７４】また、機器５１ｂ が利用権管理装置４１に利用権レコードＲrqt の新規登録を要求する場合には、上述の機器５１ａと利用権管理装置４１との間で行われたデータ通信と同様の動作が行われるので、その説明を省略する。

【０１７５】ユーザβは、機器５１ａを使って、機器５１ｂ のために生成された利用権情報Ｄrqt を使いたい場合がある。このような場合、ユーザβは、機器５１ａを操作して、コンテンツ識別子Ｉcnt を指定し、さらに、共有対象識別子Ｉdvとしての機器識別子Ｉdvb を指定する。ここで注意を要するのは、機器５１ａが、機器５１ｂ が既に設定した利用権情報Ｄrqt を共有することから、ユーザβは、利用条件Ｃcnt を特に指定する必要性が無い点である。以上の指定に応答して、機器５１ａの設定要求生成部５１１は、今回指定されたものの中に、共有対象識別子Ｉdvが含まれているか否かを判断する（ステップＳ１０１）。上述から明らかなように、今回指定されるものには、共有対象識別子Ｉdvとしての機器識別子Ｉdvbが含まれるので、設定要求生成部５１１は、図５３に示す第２の設定要求Ｄrr2aを生成し、伝送路６１を通じて、利用権管理装置４１に送信する（ステップＳ１０３）。第２の設定要求Ｄrr2aは、他の機器５１ｂ のために登録済の利用権情報Ｄrqt の共有設定を利用権管理装置４１に要求するための情報でもあり、本実施形態ではさらに、取得対象コンテンツデータＤcnt の配信を利用権管理装置４１に要求するための情報である。ステップＳ１０３をより具体的に説明すると、まず、設定要求生成部５１１は、機器識別子格納部２１１から機器識別子Ｉdva を受け取る。設定要求生成部５１１は、ユーザβが指定したコンテンツ識別子Ｉcnt および共有対象識別子Ｉdvb に、取り出した機器識別子Ｉdvａと、予め保持する設定要求識別子Ｉrrとを付加して、第２の設定要求Ｄrr2a（図５３参照）を生成する。以上の第２の設定要求Ｄrr2aは、設定要求生成部５１１から通信部２１３および伝送路６１を通じて、利用権管理装置４１に送信される。

【０１７６】利用権管理装置４１（図４９参照）において、ユーザ認証部１１６は、伝送路６１からの第２の設定要求Ｄrr2aの受信に応答して、認証処理を行い（ステップＳ１２）、その後、受け取った第２の設定要求Ｄrr2aを利用権管理部４１２に渡す。利用権管理部４１２は、ユーザ認証部１１６から第２の設定要求Ｄrr2aを受信したことに応答して、利用権ＤＢ１１４への利用権登録処理を行う（ステップＳ１０２）。ステップＳ１０２において、利用権管理部４１２は、今回、第１の設定要求Ｄrra を受信したか否かを判断する（ステップＳ１０２１）。ここで、第２の設定要求Ｄrr2aには共有対象識別子Ｉdvb が含まれるので、利用権管理部４１２は、第１の設定要求Ｄrra を受信していないと判断することになるから、ステップＳ１０２３を行う。

【０１７７】ステップＳ１０２３において、利用権管理部４１２は、受信した第２の設定要求Ｄrr2aから、共有対象識別子Ｉdvb およびコンテンツ識別子Ｉcnt を取り出す。その後、利用権管理部４１２は、利用権ＤＢ４１１にアクセスして、取り出した共有対象識別子Ｉdvb およびコンテンツ識別子Ｉcnt の双方を含む利用権レコードＲrqtaを検索する。さらに、利用権管理部４１２は、受信した第２の設定要求Ｄrr2aから機器識別子Ｉdva を取り出し、検索した利用権レコードＲrqtaに追加登録する（ステップＳ１０２４）。以上のステップＳ１０２４により、利用権ＤＢ１１４において、利用権レコードＲ

rqtaは、図５２（b'）に示すように、機器識別子Ｉdva およびＩdvb 、コンテンツ識別子Ｉcnt ならびに利用権情報Ｄrqt を含むものに更新される。これによって、コンテンツデータＤcnt の利用権情報Ｄrqtaは、機器５１ａおよび５１ｂからなるサブグループにより共有されていることが示される。以上のステップＳ１０２５が終了すると、今回受け取った第２の設定要求Ｄrr2aを、利用権管理部４１２はコンテンツ管理部１１８に渡す。以降、利用権管理装置４１は、ステップＳ１４～Ｓ１７を実行し、その後、機器５１ｂは、ステップＳ１８～Ｓ１９を実行する。また、本ライセンス情報管理システムＳｂにおいても、機器５１ａは、暗号済コンテンツデータＤecntを復号するために、ライセンス情報Ｄ1cb （第１の実施形態参照）を利用権管理装置４１から受け取る。この時、機器５１ａおよび利用権管理装置４１では、第１の実施形態で機器２１ｂおよび利用権管理装置１１が行った処理と同様に、図１１および図１２に示す処理が行われる。

【０１７８】以上のように本実施形態によれば、利用権レコードＲrqtaには、複数の機器識別子Ｉdva およびＩdvb が記録される。これによって、利用権管理装置４１は、互いに異なる機器５１ａおよび５１ｂから発行要求Ｄira およびＤirb が送信されてきたとしても、利用権レコードＲrqtaを参照することで、同一の利用権情報Ｄrqt から生成されたライセンス情報Ｄ1ca およびＤ1cb をそれらに提供することができるようになる。以上の本実施形態によって、複数の機器が共通のデジタルライツを共有できる権利管理技術を提供することができる。

【０１７９】さらに、第１の実施形態では、ユーザβが所有する複数の機器２１の１台が設定要求Ｄrrを利用権管理装置１１に送信すれば、利用権管理装置１１は、そのユーザβが所有する全機器２１の機器識別子Ｉdvを権利レコードＲrqt に一括的に登録していた。それに対して、本実施形態では、機器５１が第２の設定要求Ｄrr2を送信しない限り、利用権管理装置４１は、その送信元の機器識別子Ｉdvを権利レコードＲrqtaに登録しない。これによって、利用権情報Ｄrqt の共有をより厳密に制御することが可能となる。

【０１８０】なお、以上の第２の実施形態に係るライセンス情報管理システムＳb も、第１の実施形態に係るライセンス情報管理システムＳa と同様に、前述した第２～第５の変型例のような処理を利用権管理装置４１ならびに機器５１ａおよび５１ｂに組み込むことで、機器識別子Ｉdva および／または Ｉdvb の追加または削除が可能になる。

【０１８１】「第３の実施形態」図５４は、第３の実施形態に係るライセンス情報管理システムＳc の全体構成を示すブロック図である。図５４において、ライセンス情報管理システムＳc は、まず、少なくとも１つの利用権管理装置７１と、少なくとも１つの機器８１と、伝送路９１とを備えている。利用権管理装置７１は、コンテンツ配信に関わる事業者α側に設置される。また、機器８１は、事業者αとの契約に基づいてコンテンツ配信を受ける契約者β側に設置される。また、伝送路９１は、有線伝送路または無線伝送路であり、利用権管理装置７１および機器８１をデータ通信可能に接続する。

【０１８２】次に、図５５～図５８を参照して、図５４の利用権管理装置７１および機器８１の具体的な構成について説明する。図５５は、図５４の利用権管理装置７１の詳細な構成を示す機能ブロック図である。図５５において、利用権管理装置７１は、コンテンツデータベース７１１と、復号鍵データベース７１２と、ユーザ情報データベース７１３と、利用権データベース７１４と、通信部７１５と、ユーザ認証部７１６と、利用権管理部７１７と、コンテンツ管理部７１８と、コンテンツ暗号化部７１９と、送信データ生成部７２０と、ライセンス情報生成部７２１と、復号鍵管理部７２２と、復号鍵暗号化部７２３とを備えている。

【０１８３】また、図５６は、図５５のライセンス情報生成部７２１の詳細な構成を示す図である。図５６において、ライセンス情報生成部７２１は、ハッシュ値生成部７２１１と、ライセンス情報組立部７２１２とを含んでいる。

【０１８４】また、図５７は、図５４の機器８１の詳細な構成を示す機能ブロック図である。図５７において、機器８１は、従前の実施形態と同様の民生機器であるが、本実施形態では、便宜上、音楽再生機であると仮定して、以降の説明を続ける。以上の仮定下では、機器８１は、機器識別子格納部８１１と、設定要求生成部８１２と、通信部８１３と、コンテンツ管理部８１４と、コンテンツ蓄積部８１５と、発行要求生成部８１６と、ライセンス情報処理部８１７と、コンテンツ復号部８１８と、コンテンツ再生部８１９とを備えている。

【０１８５】また、図５８は、図５７のライセンス情報処理部８１７の詳細な構成を示す機能ブロック図である。図５８において、ライセンス情報処理部８１７は、改竄判定部８１７１と、ハッシュ値生成部８１７２と、利用許可判定部８１７３と、復号鍵復号部８１７４とを含んでいる。

【０１８６】次に、上記ライセンス情報管理システムＳc において、契約者βが事業者αからコンテンツ配信を受けるために必要となる準備について説明する。かかる準備作業では、図５５のコンテンツデータベース（以下、コンテンツＤＢと称する）７１１と、復号鍵データベース（以下、復号鍵ＤＢと称す）７１２と、ユーザ情報データベース（以下、ユーザ情報ＤＢ）７１３とが構築される。

【０１８７】まず、図５９（ａ）を参照して、図５５のコンテンツＤＢ７１１について詳細に説明する。事業者αは、図５９（ａ）に示すようなコンテンツＤＢ７１１

を構築する。より具体的には、事業者αは、契約者βに提供すべきコンテンツデータＤcnt を、自分で作成したり、別のコンテンツ制作者から受け取る。ここで、コンテンツデータＤcnt は、機器８１で利用可能なデータであって、例えば、テレビ番組、映画、ラジオ番組、音楽、書籍または印刷物を表す。また、コンテンツデータＤcnt は、ゲームプログラムまたはアプリケーションプログラムであっても良い。ただし、便宜上、本実施形態では、コンテンツデータＤcnt は音楽を表すデータであるとして、以下の説明を続ける。

【０１８８】事業者αは、以上のようにして得たコンテンツデータＤcnt のそれぞれに、コンテンツ識別子Ｉcnt を割り当てる。コンテンツ識別子Ｉcnt とは、本ライセンス情報管理システムＳc においてコンテンツデータＤcnt を一意に特定する。また、以上のコンテンツデータＤcnt は、デジタルライツを保護する観点から、利用権管理装置７１側で暗号化された上で機器８１に配信される。そのため、事業者αは、各コンテンツデータＤcnt に専用の暗号鍵Ｋe を割り当てる。以上のコンテンツ識別子Ｉcnt 、コンテンツデータＤcnt および暗号鍵Ｋe の組み合わせがコンテンツＤＢ７１１に蓄積される。したがって、図５９（ａ）に示すように、コンテンツＤＢ７１１は、コンテンツ識別子Ｉcnt 、コンテンツデータＤcntおよび暗号鍵Ｋe の組み合わせの集まりとなる。コンテンツＤＢ７１１において、コンテンツ識別子Ｉcnt は特に、同じ組みのコンテンツデータＤcnt を一意に特定する。また、暗号鍵Ｋe は、同じ組みのコンテンツデータＤcnt を暗号化するために使用される。

【０１８９】なお、以下の説明の便宜のため、図５９（ａ）に示す１つのコンテンツデータＤcnt には、一意なコンテンツ識別子Ｉcnt としての「ａ」が割り当てられると仮定する。さらに、コンテンツ識別子Ｉcnt としての「ａ」と同じ組みには、専用の暗号鍵Ｋe としての「ｂ」が登録されると仮定する。

【０１９０】また、本実施形態では、コンテンツＤＢ７１１は、コンテンツ識別子Ｉcnt 、コンテンツデータＤcnt および暗号鍵Ｋe から構成されるが、コンテンツデータＤcnt および暗号鍵Ｋe 毎のデータベースが構築されてもよい。また、コンテンツ識別子Ｉcnt は、コンテンツＤＢ７１１におけるコンテンツデータＤcnt の格納場所を特定する場合がある。かかる場合には、コンテンツＤＢ７１１に、コンテンツ識別子Ｉcnt を登録しておく必要性はない。つまり、コンテンツ識別子Ｉcnt は、コンテンツＤＢ７１１に必須の構成要素とならない。

【０１９１】次に、図５９（ｂ）を参照して、図５５の復号鍵ＤＢ７１２について詳細に説明する。上述したように、各コンテンツデータＤcnt は専用の暗号鍵Ｋe で暗号化された状態で機器８１に送信される。ここで、以下の説明において、暗号化されたコンテンツデータＤcnt を暗号済みコンテンツデータＤecntと称する。暗号済みコンテンツデータＤecntの復号のために、暗号鍵Ｋe に対応する復号鍵Ｋdが、機器８１に提供される必要がある。そのため、事業者αは、コンテンツＤＢ７１１内の各暗号鍵Ｋe に対応する復号鍵Ｋd を準備する。ここで、復号鍵Ｋdは、暗号鍵Ｋe と同じビット列からなっていてもよいし、異なるビット列からなっていてもよい。以上の復号鍵Ｋd は、上述のコンテンツ識別子Ｉcnt と共に、復号鍵ＤＢ７１２に蓄積される。以上のことから、復号鍵ＤＢ７１２は、図５９（ｂ）に示すように、コンテンツ識別子Ｉcnt および復号鍵Ｋd の組み合わせの集まりとなる。復号鍵ＤＢ７１２において、コンテンツ識別子Ｉcnt は特に、同じ組みの復号鍵Ｋd に割り当てられているコンテンツデータＤcnt を特定する。また、復号鍵Ｋd は、同じ組みのコンテンツ識別子Ｉcnt で特定される暗号済みコンテンツデータＤecntを復号するために使用される。

【０１９２】なお、以下の説明の便宜のため、図５９（ｂ）において、コンテンツ識別子Ｉcnt としての「ａ」と同じ組みには、復号鍵Ｋd として「ｃ」が登録されると仮定する。上述からも明らかであるが、復号鍵Ｋd としての「ｃ」は、暗号鍵Ｋeとしての「ｂ」による暗号済みコンテンツデータＤecntの復号に使用される。

【０１９３】次に、図６０（ａ）を参照して、図５５のユーザ情報ＤＢ７１３について詳細に説明する。上述の契約者βは、事業者αからコンテンツ配信を受けるために契約を交わす。ここで、両者の契約に関しては、契約者βが伝送路９１を通じて事業者αと行ってもよいし、他の形態で行ってもよい。この契約に基づいて、事業者αは、契約者βに機器識別子Ｉdvを割り当てる。機器識別子Ｉdvは、ライセンス情報管理システムＳc において、契約者βの機器８１を一意に特定する。以上の機器識別子Ｉdvが、ユーザ情報ＤＢ７１３に登録される。以上のことから、図６０（ａ）に示すように、ユーザ情報ＤＢ７１３は、機器識別子Ｉdvの集まりとなる。

【０１９４】ここで図５７を再度参照する。図５７に示すように、事業者αにより割り当てられた機器識別子Ｉdvはさらに、契約者β側の機器８１における機器識別子格納部８１１に設定される。機器識別子Ｉdvの設定に関しては、典型的には、事業者αが契約者β側で管理される機器８１を操作して設定する。また、他にも、事業者α側が、伝送路９１を通じて、契約者βに割り当てた機器識別子Ｉdvを送信し、機器８１が、受信した機器識別子Ｉdvを機器識別子格納部８１１に自動的に登録するようにしてもよい。

【０１９５】なお、以上の機器識別子Ｉdvは、機器８１の工場出荷時に予め、機器識別子格納部８１１に設定されていてもよい。このような場合、契約者βは、事業者αのコンテンツ配信に加入する際に、機器８１に設定されている機器識別子Ｉdvを当該事業者αに告知する。そ

して、事業者αは、告知された機器識別子ＩdvをユーザＤＢ７１３に登録する。

【０１９６】なお、以下の説明の便宜のため、図６０（ａ）に示すように、ユーザ情報ＤＢ７１３には、１つの機器識別子ＩdvとしてＩｘ１Ｉが登録されると仮定する。また、図５７に示すように、機器識別子格納部８１１には、機器識別子ＩdvとしてＩｘ１Ｉが設定されると仮定する。

【０１９７】ここで、図６０（ｂ）には、利用権データベース７１４が示されているが、当該利用権データベース７１４については、後で説明する。

【０１９８】以上の準備が終了すると、機器８１は、契約者βの操作に従って、利用権管理装置７１から、コンテンツデータＤcnt を取得することが可能となる。以下、図６１を参照して、コンテンツデータＤcnt の取得時における機器８１および利用権管理装置７１の動作について説明する。まず、契約者βは、機器８１を操作して、利用権管理装置７１にアクセスして、そのコンテンツＤＢ７１１に蓄積されているコンテンツデータＤcnt の中から、今回取得したいもののコンテンツ識別子Ｉcnt を特定する。以降の説明において、今回指定されたコンテンツデータＤcnt を、取得対象コンテンツデータＤcnt と称する。さらに、契約者βは、取得対象コンテンツデータＤcnt を利用する際の利用条件Ｃcnt を指定する。

【０１９９】以下、利用条件Ｃcnt について、より詳細に説明する。利用条件Ｃcnt は、どのような条件で、機器８１がコンテンツデータＤcnt の利用権の設定を要求するのかを示す情報である。コンテンツデータＤcnt が音楽を表す場合、利用条件Ｃcnt としては、有効期間、再生回数、最大連続再生時間、総再生時間または再生品質が代表的である。また、利用条件Ｃcnt は、有効期間、再生回数、最大連続再生時間、総再生時間および再生品質の内、２つ以上の組み合わせであってもよい。利用条件Ｃcnt としての有効期間は、例えば、２００１年６月１日から２００１年８月３１日までと設定され、設定された期間に限り、機器８１は、コンテンツデータＤcnt を再生できる。再生回数は、例えば、５回と設定され、設定された回数に限り、機器８１は、コンテンツデータＤcnt を再生できる。最大連続再生時間は、例えば、１０秒と設定され、１回の再生において設定された時間までであれば、機器８１は、コンテンツデータＤcnt を再生できる。このような最大連続再生時間は、音楽のプロモーションに特に有効である。総再生時間は、例えば、１０時間と設定され、設定された時間の範囲内であれば、機器８１は、コンテンツデータＤcnt を自由に再生できる。再生品質は、例えば、ＣＤ(CompactDisc)の品質と設定され、機器８１は、設定された再生品質でコンテンツデータＤcnt を再生できる。

【０２００】なお、上述では、コンテンツデータＤcnt が音楽を表す場合に設定されうる利用条件Ｃcnt について説明した。しかし、上述のみに限らず、利用条件Ｃcnt は、コンテンツデータＤcnt が表す内容に応じて、適切に設定されることが好ましい。また、便宜上、本実施形態では、利用条件Ｃcnt は、コンテンツデータＤcnt の再生回数であるとして、以下の説明を続ける。

【０２０１】上述したように、契約者βは、機器８１を操作して、コンテンツ識別子Ｉcntおよび利用条件Ｃcnt を指定する。このような指定に応答して、機器８１は、図６２（ａ）に示す設定要求Ｄrrを生成し、利用権管理装置７１に送信する（図６１；ステップＳ２０１）。設定要求Ｄrrは、取得対象コンテンツデータＤcnt の利用権設定を利用権管理装置７１に要求するための情報であるが、本実施形態ではさらに、取得対象コンテンツデータＤcnt の配信を利用権管理装置７１に要求するための情報でもある。ステップＳ２０１をより具体的に説明すると、まず、設定要求生成部８１２（図５７参照）は、契約者βが指定したコンテンツ識別子Ｉcnt および利用条件Ｃcnt を受け取る。また、設定要求生成部８１２は、機器識別子格納部８１１から機器識別子Ｉdv を受け取る。その後、設定要求生成部８１２は、以上の機器識別子Ｉdv、コンテンツ識別子Ｉcnt および利用条件Ｃcntに、予め保持する設定要求識別子Ｉrrを付加して、設定要求Ｄrr（図６２（ａ）参照）を生成する。ここで、設定要求識別子Ｉrrは、利用権管理装置７１が設定要求Ｄrrを特定するために使用される。設定要求生成部８１２は、以上の設定要求Ｄrrを通信部８１３に渡す。通信部８１３は、受け取った設定要求Ｄrrを、伝送路９１を通じて、利用権管理装置７１に送信する。

【０２０２】利用権管理装置７１（図５５参照）において、通信部７１５は、伝送路９１を通じて送信されてくる設定要求Ｄrrを受信して、ユーザ認証部７１６に渡す。ユーザ認証部７１６は、設定要求Ｄrrを受け取ると、ユーザ認証処理を行う（図６１：ステップＳ２０２）。より具体的には、ユーザ認証部７１６は、上述のユーザ情報ＤＢ７１３（図６０（ａ）参照）を管理しており、受け取った設定要求Ｄrrに設定されている機器識別子Ｉdvに一致するものが、当該ユーザ情報ＤＢ７１３に登録されているか否かを確認する。ユーザ認証部７１６は、ユーザ情報ＤＢ７１３に一致するものが登録されている場合に限り、今回設定要求Ｄrrが、契約者βの機器８１から送信されてきたものであると判断する。ユーザ認証部７１６は、以上のユーザ認証が終了すると、受け取った設定要求Ｄrrを利用権管理部７１７に渡す。

【０２０３】なお、正規の契約者β以外からの設定要求Ｄrrを受け取った場合、ユーザ認証部７１６は、ユーザ認証に失敗する。かかる場合、ユーザ認証部７１６は、当該設定要求Ｄrrを利用権管理部７１７に渡すことなく、当該設定要求Ｄrrを廃棄する。

【０２０４】利用権管理部７１７（図５５参照）は、利

用権データベース（以下、利用権ＤＢと称する）７１４を管理している。また、利用権管理部７１７は、そこに設定されている設定要求識別子Ｉrrに基づいて、ユーザ認証部７１６から設定要求Ｄrrを渡されれたことを認識する。このような認識結果に従って、利用権管理部７１７は、利用権ＤＢ７１４への利用権登録処理を行う（ステップＳ２０３）。より具体的には、利用権管理部７１７は、設定要求Ｄrrから、機器識別子Ｉdv、コンテンツ識別子Ｉcnt および利用条件Ｃcnt を取り出して、それらの組み合わせを利用権ＤＢ７１４に登録する。ここで、利用権管理部７１７は、設定要求Ｄrrに設定されている利用条件Ｃcnt で、機器８１が取得対象コンテンツデータＤcnt を利用する権利を要求しているとみなす。つまり、利用権管理部７１７からみれば、利用条件Ｃcnt は、取得対象コンテンツデータＤcnt を機器８１が利用できる権利を示す。以上の観点から、利用権管理部７１７は、設定要求Ｄrrから取り出した利用条件Ｃcnt を、機器８１が設定要求している利用権情報Ｄrqt として扱う。つまり、利用権ＤＢ７１４は、図６０（ｂ）に示すように、機器識別子Ｉdv、コンテンツ識別子Ｉcnt および利用権情報Ｄrqt の組み合わせの集まりとなる。これによって、利用権管理部７１７は、契約者βｊ毎に、取得対象コンテンツデータＤcnt の利用権を管理する。利用権管理部７１７は、以上の利用条件登録処理が終了すると、今回受け取った設定要求Ｄrrをコンテンツ管理部７１８に渡す。

【０２０５】ここで、以上の利用権ＤＢ７１４に登録される利用権情報Ｄrqt の具体例について説明する。既に説明している通り、本実施形態では、利用条件Ｃcnt は利用回数であると仮定されている。さらに、今回の設定要求Ｄrrには、機器識別子Ｉdvとして「ｘｉ」、コンテンツ識別子Ｉcnt として「ａ」および利用条件Ｃcntとして「再生ｍ回」（ｍは自然数）が設定されていると仮定する。以上の仮定下では、図６０（ｂ）に示すように、機器識別子Ｉdvとしての「ｘｉ」、コンテンツ識別子Ｉcnt としての「ａ」および利用権情報Ｄrqt としての「再生ｍ回」の組み合わせが設定される。

【０２０６】なお、本ライセンス情報管理システムＳｃの技術的特徴とは関係ないが、ステップＳ２０３において、利用権管理部７１７は、利用権情報Ｄrqt の登録毎に、機器識別子Ｉdvが割り当てられている契約者βｊに対して課金を行ってもよい。

【０２０７】コンテンツ管理部７１８は、設定要求Ｄrrを受け取ると、コンテンツデータＤcnt の読み出し処理を行う（ステップＳ２０４）。より具体的には、コンテンツ管理部７１８は、受け取った設定要求Ｄrrから、コンテンツ識別子Ｉcnt を取り出す。その後、コンテンツ管理部７１８は、コンテンツＤＢ７１１にアクセスして、取り出したコンテンツ識別子Ｉcnt が割り当てられているコンテンツデータＤcnt および暗号鍵Ｋｅを読み出す。以上の読み出し処理が終了すると、コンテンツ管理部７１８は、読み出したコンテンツデータＤcnt および暗号鍵Ｋｅをコンテンツ暗号化部７１９に渡す。さらに、コンテンツ管理部７１８は、受け取った設定要求Ｄrrを送信データ生成部７２０に渡す。

【０２０８】コンテンツ暗号化部７１９は、コンテンツデータＤcnt の暗号処理を行う（ステップＳ２０５）。より具体的には、コンテンツ暗号化部７１９は、受け取ったコンテンツデータＤcnt を、それと同時に受け取った暗号鍵Ｋｅで暗号化して、前述の暗号済みコンテンツデータＤecntを生成する。コンテンツ暗号化部７１９は、以上の暗号処理が終了すると、暗号済みコンテンツデータＤecntを送信データ生成部７２０に渡す。

【０２０９】送信データ生成部７２０は、コンテンツ管理部７１８からの設定要求Ｄrrと、コンテンツ暗号化部７１９からの暗号済みコンテンツデータＤecntとが揃うと、送信データ生成処理を行う（ステップＳ２０６）。より具体的には、送信データ生成部７２０は、受け取った設定要求Ｄrrから、コンテンツ識別子Ｉcnt を取り出す。さらに、送信データ生成部７２０は、取り出したコンテンツ識別子Ｉcntを、受け取った暗号済みコンテンツデータＤecntに付加して、図６２（ｂ）に示すような、送信データＤtrn を生成する。送信データ生成部７２０は、以上の送信データ生成処理が終了すると、送信データＤtrn を通信部７１５に渡す。通信部７１５は、受け取った送信データＤtrn を、伝送路９１を介して、機器８１へと送信する（ステップＳ２０７）。

【０２１０】機器８１（図５７参照）において、通信部８１３は、伝送路９１を通じて送信されてくる送信データＤtrn を受信する（ステップＳ２０８）。より具体的には、通信部８１３は、それに含まれるコンテンツ識別子Ｉcnt から、今回、送信データＤtrn を受信したことを認識する。このような認識結果に従って、通信部８１３は、受信データＤtrn をコンテンツ管理部８１４に渡す。

【０２１１】コンテンツ管理部８１４は、受信データＤtrn 内のコンテンツ識別子Ｉcnt および暗号済みコンテンツデータＤecntを、コンテンツ蓄積部８１５に蓄積する（ステップＳ２０９）。つまり、コンテンツ蓄積部８１５には、図６３に示すように、上述の設定要求Ｄrrにより要求されたコンテンツ識別子Ｉcnt および暗号済みコンテンツデータＤecntの組み合わせが、いくつか蓄積されることになる。

【０２１２】デジタルライツの保護の観点から、機器８１には暗号済みコンテンツデータＤecntが配信される。そのため、機器８１は、コンテンツデータＤcnt を利用する場合には、利用権管理装置７１により提供される復号鍵Ｋｄで、暗号済みコンテンツデータＤecntを復号する必要がある。ここで、本ライセンス情報管理システムＳｃでは、復号鍵Ｋｄを機器８１に提供するために、後

で詳説するライセンス情報Ｄｌｃが用いられる。以下、図６４～図６６を参照して、ライセンス情報Ｄｌｃの取得およびコンテンツデータＤｃｎｔの復号時における機器８１および利用権管理装置７１の動作について説明する。

【０２１３】まず、契約者βは、機器８１を操作して、コンテンツ蓄積部８１５にアクセスして、そこに蓄積されている暗号済みコンテンツデータＤｅｃｎｔの中から、今回利用したいものを特定する。ここで、以下の説明において、今回指定された暗号済みコンテンツデータＤｅｃｎｔを、復号対象コンテンツデータＤｅｃｎｔと称する。

【０２１４】以上の契約者βによる指定に応答して、機器８１は、図６７（ａ）に示すような発行要求Ｄｉｒを生成し、利用権管理装置７１に送信する（図６４；ステップＳ３０１）。発行要求Ｄｉｒは、上述のライセンス情報Ｄｌｃの提供を利用権管理装置７１に要求するため、つまり復号対象コンテンツデータＤｅｃｎｔの利用許可を受けるための情報である。より具体的にステップＳ３０１を説明すると、コンテンツ管理部８１４（図５７参照）は、コンテンツ蓄積部８１５を管理しており、契約者βにより特定された復号対象コンテンツデータＤｅｃｎｔに付加されているコンテンツ識別子Ｉｃｎｔを、当該コンテンツ蓄積部８１５から取り出す。発行要求生成部８１６は、コンテンツ管理部８１４により取り出されたコンテンツ識別子Ｉｃｎｔを受け取る。さらに、発行要求生成部８１６は、機器識別子格納部８１１から機器識別子Ｉｄｖを受け取る。その後、発行要求生成部８１６は、機器識別子Ｉｄｖおよびコンテンツ識別子Ｉｃｎｔに、発行要求識別子Ｉｉｒを付加して、発行要求Ｄｉｒ（図６７（ａ）参照）を生成する。ここで、発行要求識別子Ｉｉｒは、利用権管理装置７１が発行要求Ｄｉｒを特定するために使用される。発行要求生成部８１６は、以上の発行要求Ｄｉｒを通信部８１３に渡す。通信部８１３は、受け取った発行要求Ｄｉｒを伝送路９１を通じて、利用権管理装置７１に送信する。

【０２１５】利用権管理装置７１において、通信部７１５（図５５参照）は、伝送路９１を通じて送信されてくる発行要求Ｄｉｒを受信して、ユーザ認証部７１６に渡す。

【０２１６】ユーザ認証部７１６は、発行要求Ｄｉｒを受け取ると、ユーザ認証処理を行う（ステップＳ３０２）。より具体的には、ユーザ認証部７１６は、受け取った発行要求Ｄｉｒから、機器識別子Ｉｄｖを取り出す。この後、ユーザ認証部７１６は、ステップＳ２０２（図６１参照）と同様にして、今回の発行要求Ｄｉｒに認証処理を行った後に、当該発行要求Ｄｉｒを利用権管理部７１７に渡す。

【０２１７】利用権管理部７１７は、それに設定されている発行要求識別子Ｉｉｒに基づいて、今回、ユーザ認証部７１６から発行要求Ｄｉｒを渡されたことを認識する。このような認識結果に従って、利用権管理部７１７は、受け取った発行要求Ｄｉｒから、機器識別子Ｉｄｖおよびコンテンツ識別子Ｉｃｎｔを取り出す（ステップＳ３０３）。次に、利用権管理部７１７は、取り出した機器識別子Ｉｄｖおよびコンテンツ識別子Ｉｃｎｔの組み合わせが、利用権ＤＢ７１４（図６０（ｂ）参照）に登録されているか否かを判断する（ステップＳ３０４）。

【０２１８】利用権管理部７１７は、ステップＳ３０４で「Ｙｅｓ」と判断した場合、それらと同じ組みの利用権情報Ｄｒｑｔを参照して、機器８１に利用許可を与えることができるか否かを判断する（ステップＳ３０５）。ステップＳ３０５で「Ｙｅｓ」と判断した場合、利用権管理部７１７は、利用権情報Ｄｒｑｔの一部または全てを取り出す（ステップＳ３０６）。ここで、以下の説明において混同が生じることを避けるため、ステップＳ３０６において取り出された一部または全ての利用権情報Ｄｒｑｔのことを、今回の発行要求Ｄｉｒにより特定される機器８１にコンテンツデータＤｃｎｔの利用を許可するための情報であるという観点から、利用許可情報Ｄｌｗと称する。つまり、ステップＳ３０６では、利用許可情報Ｄｌｗが生成される。

【０２１９】利用許可情報Ｄｌｗの生成により、機器８１のために登録されている利用権情報Ｄｒｑｔの一部または全てが使用される。そのため、ステップＳ３０６の次に、利用権管理部７１７は、ステップＳ３０６で一部または全部が取り出された利用権情報Ｄｒｑｔを更新する（ステップＳ３０７）。

【０２２０】ここで、以上のステップＳ３０３～Ｓ３０７の処理の具体例について説明する。今、利用権ＤＢ７１４には、図６０（ｂ）に示すように、機器識別子Ｉｄｖとしての「ｘ１」、コンテンツ識別子Ｉｃｎｔとしての「ａ」および利用権情報Ｄｒｑｔとしての「再生ｍ回」の組みが登録されていると仮定する。また、今回、機器８１は、機器識別子Ｉｄｖとしての「ｘ１」およびコンテンツ識別子Ｉｃｎｔとしての「ａ」が設定されている発行要求Ｄｉｒを送信すると仮定する。

【０２２１】以上の仮定下では、ステップＳ３０３において、発行要求Ｄｉｒから、機器識別子Ｉｄｖとしての「ｘ１」と、コンテンツ識別子Ｉｃｎｔとしての「ａ」が取り出される。また、ステップＳ３０４において、機器識別子Ｉｄｖとしての「ｘ１」およびコンテンツ識別子Ｉｃｎｔとしての「ａ」の組みが、利用権ＤＢ７１４に登録されていると判断される。このように判断されると、ステップＳ３０５において、同じ組みの利用権情報Ｄｒｑｔには、「再生ｍ回」と設定されているので、機器８１の利用許可を与えてもよいと判断される。このように判断されると、ステップＳ３０６において、利用許可情報Ｄｌｗが生成される。この時生成される利用許可情報Ｄｌｗとしては、例えば、「再生ｎ回」が挙げられる。ここで、ｎは、上述のｍを超えない自然数であり、より好ましくは、機器８１の処理能力に応じて設定される。例えば、

機器８１が相対的に低い性能のハードウェアを搭載している場合であれば、ｎは、「１」のように、機器８１が復号対象コンテンツデータＤecntを利用可能な最低限の値に設定されることが好ましい。

【０２２２】以上のステップＳ３０３～Ｓ３０６により、機器８１（機器識別子Ｉdv「ｘ１」）がコンテンツデータＤcnt（コンテンツ識別子Ｉcnt「ａ」）を再生する権利をｎ回使うことになる。そのため、ステップＳ３０７において、利用権情報Ｄrqt が「再生ｍ回」から「再生（ｍ－ｎ）回」に更新される。

【０２２３】以上の具体例では、利用権情報Ｄrqt がコンテンツデータＤcnt の再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムＳｃでは、様々な利用権情報Ｄrqt（つまり利用条件Ｃcnt）を設定することができる。従って、ステップＳ３０３からＳ３０７までの処理手順は、利用権情報Ｄrqtに応じて適切に規定される必要がある。

【０２２４】以上のようにして生成した利用許可情報Ｄ１wを、利用権管理部７１７（図５５参照）は、発行要求Ｄirと一緒に、ライセンス情報生成部７２１に渡す。より具体的には、ライセンス情報生成部７２１は、図５６に示すように、ハッシュ値生成部７２１１およびライセンス情報組立部７２１２を含んでいる。ハッシュ値生成部７２１１には、利用許可情報Ｄ１wのみが渡され、また、ライセンス情報組立部７２１２には、利用許可情報Ｄ１wおよび発行要求Ｄirの双方が渡される。

【０２２５】まず、ハッシュ値生成部７２１１は、予め保持するハッシュ関数ｆ（ｘ）に、受け取った利用許可情報Ｄ１wを代入して、利用許可情報Ｄ１wの改竄を防止するするためのハッシュ値Ｖhsを生成する（ステップＳ３０８）。つまり、ハッシュ値Ｖhsは、利用許可情報Ｄ１wを生成多項式ｆ（ｘ）に代入した時に得られる解である。以上のようなハッシュ値Ｖhsを、ハッシュ値生成部７２１１は、ライセンス情報組立部７２１２に渡す。

【０２２６】ライセンス情報組立部７２１２は、受け取った発行要求Ｄirを復号鍵管理部７２２に渡す。復号鍵管理部７２２（図５５参照）は、前述した復号鍵ＤＢ７１２（図５９（ｂ）参照）を管理する。復号鍵管理部７２２は、受け取った発行要求Ｄirに設定されているコンテンツ識別子Ｉcnt および機器識別子Ｉdvを取り出す。さらに、復号鍵管理部７２２は、コンテンツ識別子Ｉcntと同じ組みの復号鍵Ｋｄを復号鍵ＤＢ７１２から取り出して、機器識別子Ｉdvと一緒に復号鍵暗号化部７２３に渡す。復号鍵暗号化部７２３は、受け取った復号鍵Ｋｄを、同時に受け取った機器識別子Ｉdvで暗号化して（ステップＳ３０９）、暗号済みの復号鍵Ｋedを生成する。以上の暗号済み復号鍵Ｋedは、ライセンス情報組立部７２１２に渡される。

【０２２７】ライセンス情報組立部７２１２は、発行要求Ｄirおよび利用許可情報Ｄ１w、ハッシュ値Ｖhsならびに暗号済み復号鍵Ｋedのすべてが揃うと、図６７（ｈ）に示すライセンス情報Ｄ１cの生成を開始する（図６５：ステップＳ３０１０）。より具体的には、ライセンス情報組立部７２１２は、発行要求Ｄirから、コンテンツ識別子Ｉcnt を取り出して、利用許可情報Ｄ１w、暗号済み復号鍵Ｋedおよびハッシュ値Ｖhsに付加する。さらに、ライセンス情報組立部７２１２は、予め保持するライセンス情報識別子Ｉ１cを、コンテンツ識別子Ｉcnt に付加して、ライセンス情報Ｄ１cを生成する。以上のライセンス情報Ｄ１cは、復号対象コンテンツデータＤecntの機器８１における利用を制御するための情報である。また、ライセンス情報識別子Ｉ１cは、機器８１がライセンス情報Ｄ１cを特定するための情報である。また、以上のライセンス情報Ｄ１cは、通信部７１５に渡される。通信部７１５から、伝送路９１を通じて、機器８１に送信される（ステップＳ３０１１）。

【０２２８】機器８１（図５７参照）において、通信部８１３は、伝送路９１を通じて送信されてくるライセンス情報Ｄ１cを受信する（ステップＳ３０１２）。より具体的には、通信部８１３は、それに設定されるライセンス情報識別子Ｉ１cから、今回、ライセンス情報Ｄ１cを受け取ったことを認識する。このような認識結果に従って、通信部８１３は、受け取ったライセンス情報Ｄ１cをライセンス情報処理部８１７に渡す。

【０２２９】ライセンス情報処理部８１７は、図５８に示すように、改竄判定部８１７１と、ハッシュ値生成部８１７２と、利用許可判定部８１７３と、復号鍵復号部８１７４とを含んでいる。通信部８１３からのライセンス情報Ｄ１cは、まず、改竄判定部８１７１に渡される。改竄判定部８１７１は、まず、受け取ったライセンス情報Ｄ１cから、利用許可情報Ｄ１wおよびハッシュ値Ｖhsを取り出し（ステップＳ３０１３）、取り出した利用許可情報Ｄ１wを、ハッシュ値生成部８１７２に渡し、ハッシュ値Ｖhsをそのまま保持する。ここで、以下の説明において混同が生じないように、ステップＳ３０１３で取り出されたハッシュ値Ｖhsを、機器８１の外部（つまり利用権管理装置７１）で生成されたものであるという観点から、外部ハッシュ値Ｖehs と称する。

【０２３０】ハッシュ値生成部８１７２は、利用権管理装置７１側のハッシュ値生成部７２１１（図３参照）と同じハッシュ関数ｆ（ｘ）を保持しており、受け取った利用許可情報Ｄ１wをハッシュ関数ｆ（ｘ）に代入してハッシュ値Ｖhsを生成する（ステップＳ３０１４）。ここでステップＳ３０１４で生成されたハッシュ値Ｖhsを、機器８１の内部で生成されたものであるという観点から、内部ハッシュ値Ｖ１hs と称する。ハッシュ値生成部８１７２は、以上の内部ハッシュ値Ｖ１hs を、改竄判定部８１７１に返す。

【０２３１】改竄判定部８１７１は、上述の内部ハッシュ値Ｖ１hs を受け取ると、利用許可情報Ｄ１wが改竄され

ているか否かを判定する（ステップＳ３０１５）。より具体的には、上述の内部ハッシュ値Ｖ1hs は、ライセンス情報Ｄ1c内の利用許可情報Ｄ1wが改竄されていないという条件で、外部ハッシュ値Ｖehs に一致する。そこで、ステップＳ３０１５において、改竄判定部８１７１は、受け取った内部ハッシュ値Ｖ1hs が外部ハッシュ値Ｖehs に一致するか否かを判定する。改竄判定部８１７１は、「Ｙｅｓ」と判定した場合には、利用許可情報Ｄ1wが改竄されておらず、今回送信されてきた利用許可情報Ｄ1wが有効であるとみなして、今回受け取ったライセンス情報Ｄ1cを利用許可判定部８１７３に渡す。

【０２３２】利用許可判定部８１７３は、受け取ったライセンス情報Ｄ1cを参照して、復号対象コンテンツデータＤecntの利用が許可されているか否かを判定する（ステップＳ３０１６）。利用許可判定部８１７３は、ステップＳ３０１６において「Ｙｅｓ」と判断した場合に限り、受け取ったライセンス情報Ｄ1cから、暗号済み復号鍵Ｋedを取り出して、復号鍵復号部８１７４に渡す。

【０２３３】ここで、以上のステップＳ３０１６の処理の具体例について説明する。前述の仮定に従えば、今回のライセンス情報Ｄ1cの利用許可情報Ｄ1wにより、コンテンツデータＤcnt の再生がｎ回だけ許可されている。かかる場合、利用許可判定部８１７３は、ステップＳ３０１６において、利用許可情報Ｄ1wに設定される再生回数が１以上であれば、復号対象コンテンツデータＤecntの利用が許可されていると判断して、受け取ったライセンス情報Ｄ1cから暗号済み復号鍵Ｋedを取り出して、復号鍵復号部８１７４に渡す。

【０２３４】以上の具体例では、利用権情報Ｄrat がコンテンツデータＤcnt の再生回数であるとして説明したが、前述したように、本ライセンス情報管理システムＳｃでは、様々な利用権情報Ｄrat （つまり利用条件Ｃcnt ）を設定することができる。従って、ステップＳ３０１６の処理は、利用権情報Ｄrat に応じて適切に規定される必要がある。

【０２３５】さて、復号鍵復号部８１７４は、利用許可判定部８１７３から暗号済み復号鍵Ｋedを受け取る。さらに、復号鍵復号部８１７４は、機器識別子格納部８１１から機器識別子Ｉdvを受け取る。その後、復号鍵復号部８１７４は、暗号済み復号鍵Ｋedを、機器識別子Ｉdv で復号して（ステップＳ３０１７）、復号鍵Ｋd をコンテンツ復号部８１８に渡す。

【０２３６】ところで、コンテンツ管理部８１４は、ステップＳ３０１において、コンテンツ識別子Ｉcnt だけでなく、前述の復号対象コンテンツデータＤecntを取り出す。取り出された復号対象コンテンツデータＤecnt は、コンテンツ復号部８１８に渡される。コンテンツ復号部８１８は、復号鍵復号部８１７４から受け取った復号鍵Ｋd で、復号対象コンテンツデータＤecntを復号して（ステップＳ３０１８）、コンテンツデータＤcnt をコンテンツ再生部８１９に渡す。コンテンツ再生部８１９は、受け取ったコンテンツデータＤcnt を再生して、音声出力する（ステップＳ３０１９）。これにより、契約者βは、事業者αから購入したコンテンツデータＤcnt が表す音楽を聴くことができる。

【０２３７】ここで、図６５のステップＳ３０１５を参照する。ステップＳ３０１５において、改竄判定部８１７１は、利用許可情報Ｄ1wが改竄されていると判定する場合がある。また、ステップＳ３０１６において、利用許可判定部８１７３は、復号対象コンテンツデータＤecntの利用が許可されていないと判定する場合もある。このような場合、改竄判定部８１７１および利用許可判定部８１７３は、今回受け取ったライセンス情報Ｄ1cを破棄する（図６６；ステップＳ３０２０）。以上から明らかなように、本ライセンス情報管理システムＳｃ では、有効なライセンス情報Ｄ1cを受信した場合にのみ、復号対象コンテンツデータＤecntの復号が許可される。これによって、上述のデジタルライツが保護される。

【０２３８】ここで、図６４のステップＳ３０４において、利用権管理部７１７は、機器識別子Ｉdvおよびコンテンツ識別子Ｉcnt の組み合わせが、利用権ＤＢ７１４（図６０（ｂ）参照）に登録されていないと判断する場合がある。さらに、ステップＳ３０５において、利用権管理部７１７は、機器８１に利用許可を与えないと判断する場合もある。このような場合、利用権管理部７１７は、復号対象コンテンツデータＤecntの利用を拒否することを示す利用拒否情報Ｄrj（図６７（ｃ）参照）を生成して、通信部７１５に渡す。通信部７１５は、受け取った利用拒否情報Ｄrjを、伝送路９１を介して、機器８１に送信する（図６６；ステップＳ３０２１）。

【０２３９】機器８１（図５７参照）において、通信部８１３は、伝送路９１を通じて送信されてくる利用拒否情報Ｄrjを受信する（ステップＳ３０２２）。利用拒否情報Ｄrjの受信以降、機器８１では何の処理も行われない。以上から明らかなように、本ライセンス情報管理システムＳｃ では、利用権ＤＢ７１４に有効な機器識別子Ｉdv、コンテンツ識別子Ｉcnt および利用権情報Ｄrat の組み合わせが登録されてない場合には、利用拒否情報Ｄrjが機器８１に送信される。これによって、機器８１側では、復号対象コンテンツデータＤecntは復号されない。これによって、上述のデジタルライツが保護される。

【０２４０】なお、ステップＳ３０４において、利用権管理部７１７は、機器識別子Ｉdvおよびコンテンツ識別子Ｉcnt の組み合わせが、利用権ＤＢ７１４（図６０（ｂ）参照）に登録されていないと判断する場合、機器識別子Ｉdv、コンテンツ識別子Ｉcnt および利用権情報Ｄrat の組み合わせを新しく生成して、当該利用権ＤＢ７１４に登録するようにしてもよい。

【０２４１】以上説明したように、本ライセンス情報管

理システムＳｃでは、各コンテンツデータＤcntを機器８１が利用するための権利を表す利用権情報Ｄratを利用権管理装置７１側で一元的に管理できるようになる。そのため、以上のような利用権情報Ｄratを管理するための処理負担を機器８１に負わせる必要がなくなる。これによって、本ライセンス情報管理システムＳｃによれば、処理能力の低い民生機器に適した権利保護技術を提供することができる。

【０２４２】なお、以上の実施形態では、同じ事業者αにより管理される利用権管理装置７１が、図６１の処理および図６４～図６６の処理の双方を行うとして説明した。しかしながら、互いに異なる利用権管理装置が図６１の処理と図６４～図６６の処理とを行うようにしてもよい。つまり、ある事業者により管理される利用権管理装置がコンテンツデータＤcntの配信を担当し、他の事業者により管理される利用権管理装置がライセンス情報Ｄ１cの提供を担当するように、本ライセンス情報管理システムＳｃは構成されてもよい。さらに、説明の便宜のため、本実施形態では、最初に、コンテンツデータＤcntの取得（図６１の処理）が行われ、その後に、ライセンス情報Ｄ１cの取得（図６４～図６６の処理）が行われていた。しかしながら、最初にライセンス情報Ｄ１cの取得が行われ、その後に、コンテンツデータＤcntの取得が行われても良い。また、コンテンツデータＤcntの取得およびライセンス情報Ｄ１cの取得が同時並行して行われてもよい。

【０２４３】また、以上の実施形態では、コンテンツＤＢ１１４は、暗号化されていないコンテンツデータＤcntおよび暗号鍵Ｋｅの集まりであった。利用権管理装置７１は、送信データＤtrnの生成直前に、コンテンツデータＤcntを暗号鍵Ｋｅで暗号化するようにしていた（ステップＳ２０５参照）。しかしながら、コンテンツデータＤcntの暗号化に要する処理時間を削減するために、コンテンツＤＢ１１４は、前述の暗号済みコンテンツデータＤecntの集まりであってもよい。この場合、利用権管理装置７１は、設定要求Ｄrrに設定されるコンテンツ識別子Ｉcntが示す暗号済みコンテンツデータＤecntに、当該コンテンツ識別子Ｉcntを付加して送信データＤtmを生成し送信する。

【０２４４】また、以上の実施形態では、ライセンス情報生成部７２１において、ハッシュ値生成部７２１１は、利用許可情報Ｄ１wのみからハッシュ値Ｖhsを生成していた。しかし、これに限らず、以下のようにしてハッシュ値Ｖhsを生成してもよい。まず、ライセンス情報組立部７２１２は、ライセンス情報Ｄ１cの構成要素であるライセンス情報識別子Ｉ１c、コンテンツ識別子Ｉcnt、利用許可情報Ｄ１w、および暗号済み復号鍵Ｋedの内のいずれか、もしくは２つ以上をハッシュ値生成部７２１１に渡す。ハッシュ値生成部７２１１は、ライセンス情報組立部７２１２から受け取ったものを、上述のハッシュ関数ｆ（ｘ）に代入して、ハッシュ値Ｖhsを生成する。

【０２４５】また、以上の実施形態では、ライセンス情報Ｄ１cは、暗号済み復号鍵Ｋedを含んでいた。しかし、これに限らず、ライセンス情報Ｄ１cは、復号鍵Ｋｄを含んでいてもよい。この場合、伝送路９１上で、第三者に復号鍵Ｋｄが盗まれる危険があるので、ＳＳＬ(Secure Socket Layer)に代表される技術を用いて、利用権管理装置７１から機器８１へと伝送されるライセンス情報Ｄ１cを保護することが好ましい。さらに、ＳＳＬだけでは、機器８１において、ライセンス情報Ｄ１cがそのままの状態で保持される。このような状況では、機器８１から他の機器へとライセンス情報Ｄ１cが転送されれば、当該他の機器は、ライセンス情報Ｄ１cを利用できるので、デジタルライツの保護という観点からは好ましくない。そのため、機器識別子格納部８１１に格納される機器識別子Ｉdvでライセンス情報Ｄ１cを暗号化するアルゴリズムを、機器８１に組み込むことがより好ましい。これにより、ライセンス情報Ｄ１cは機器８１以外では使用できなくなるので、デジタルライツを保護することが可能となる。

【０２４６】また、以上の実施形態では、説明の便宜上、ユーザ情報ＤＢ７１３には、機器識別子Ｉdvのみが登録されるとして説明した。しかしながら、ユーザ情報ＤＢ７１３にはさらに、契約者βを一意に特定可能な他のユーザ情報（例えば、住所および電話番号）が登録されてもよい。また、以上のような複雑なユーザ情報で復号鍵Ｋｄを暗号化するようにしてもよい。これによって、復号鍵Ｋｄの暗号強度が高くなるので、より好ましくデジタルライツを保護できるライセンス情報管理システムＳｃを提供することが可能となる。

【０２４７】また、以上の実施形態では、説明の便宜上、コンテンツデータＤcntが音楽データであるとして説明した。そのため、機器８１は、コンテンツ再生部８１９を含んでおり、当該コンテンツ再生部８１９は、復号されたコンテンツデータＤcntを再生して、音声を出力するとして説明した。しかしながら、前述したように、コンテンツデータＤcntは、機器８１で利用可能なデータであればよく、当該コンテンツデータＤcntが表すのは、テレビ番組、映画、ラジオ番組、書籍、印刷物、ゲームプログラムまたはアプリケーションプログラム等、多岐にわたる。したがって、コンテンツ再生部８１９は、音声出力するものに限らず、コンテンツデータＤcntの種類に応じて、テレビ番組、映画、書籍および印刷物およびゲーム内容を映像出力可能なもの、ラジオ番組を音声出力可能なものに置換されてもよい。さらに、機器８１は、以上のようなコンテンツ再生部８１９に代えて、復号されたコンテンツデータＤcntを、外部の機器（テレビジョン受像機、ラジオ受信機、音楽再生機、電子ブックリーダ、ゲーム機器、ＰＣ、情報携帯端末、携帯電話、外部記憶装置等）に転送可能なインター

フェイスを備えていてもよい。

【０２４８】ところで、以上のライセンス情報管理システムＳｃにおいて、事業者αは、契約者βにコンテンツ配信を提供する。しかしながら、上述のライセンス情報管理システムＳｃでは、機器８１に機器識別子Ｉdvが固定的に設定されてしまうため、契約者βが、同じ事業者αと契約している宿泊施設において、自分の利用権情報Ｄrqtを使ってコンテンツデータＤcntを、当該宿泊施設に設置された機器８１で利用することができないという問題点があった。また、同様の理由で、ある契約者βが、同じ事業者αと契約している知人宅において、自分の利用権情報Ｄrqtを使って、コンテンツデータＤcntを利用することができないという問題点があった。以下の第６の変形例に係るライセンス情報管理システムＳc1は、以上のような問題点を解決して、より使い勝手のよいコンテンツ配信を実現することを目的とする。

【０２４９】「第６の変型例」図６８は、ライセンス情報管理システムＳc1の全体構成を示すブロック図である。図６８のライセンス情報管理システムＳc1は、図５４のライセンス情報管理システムＳｃと比較すると、可搬型記録媒体１０１および機器２０１とをさらに備える点で相違する。この点以外に両システムＳｃおよびＳc1の間に構成面での相違は無いので、図６８において、図５４のライセンス情報管理システムＳｃに相当する構成には同一の参照符号を付し、その説明を簡素化する。つまり、以下において、利用権管理装置７１および機器８１の説明を行う場合には、図５５～図５７を援用する。

【０２５０】可搬型記録媒体１０１は、代表的には、ＳＤカードやスマートメディア（いずれも商標）のように、契約者βが携帯可能な種類の記録媒体であって、図６９に示すように、自身を一意に特定するメディア識別子Ｉmdを、予め定められた記録領域に格納している。ここで、本実施形態では、便宜上、図６９に示すように、メディア識別子Ｉmdは「ｘ２」であるとして、以下の説明を続ける。以上の可搬型記録媒体１０１は、前述の機器８１と同じ契約者βにより管理される。

【０２５１】機器２０１は、事業者αとの契約に基づいてコンテンツ配信を受ける契約者γ側に設置される。ここで、契約者γは、本実施形態では、上述したような宿泊施設を所有しており、機器２０１は、当該宿泊施設に設置される。以下、機器２０１の詳細な構成を説明する。

【０２５２】ここで、図７０は、図６８の機器２０１の詳細な構成を示す機能ブロック図である。図７０において、機器２０１は、機器８１と同様の民生機器が代表的であるが、本実施形態では、便宜上、音楽再生機であると仮定して、以降の説明を続ける。以上の仮定下では、機器２０１は、上述の可搬型記録媒体１０１を装着可能に構成されており、図５７に示す機器８１と比較すると、インターフェイス２０２１と、識別子抽出部２０２２とをさらに備える点で相違する。この点以外に両機器２０１および８１の間に構成面での相違は無いので、図７０の機器２０１において、図５７の機器８１に相当する構成には同一の参照符号を付し、その説明を簡素化する。

【０２５３】次に、上記ライセンス情報管理システムＳc1において、契約者βが、自分の利用権情報Ｄrqtを使って、他者（つまり、契約者γ）側の機器２０１上で事業者αからコンテンツ配信を受けるために必要となる準備について説明する。かかる準備作業では、前述の実施形態と同様に、まず、図５５のコンテンツデータベース（以下、コンテンツＤＢと称する）７１１と、復号鍵データベース（以下、復号鍵ＤＢと称す）７１２と、ユーザ情報データベース（以下、ユーザ情報ＤＢ）７１３とが構築される。なお、コンテンツＤＢ７１１および復号鍵ＤＢ７１２については、図５９（ａ）および同図（ｂ）を参照して前述した通りであるため、本変形例では、それぞれの説明を省略する。

【０２５４】しかしながら、ユーザ情報ＤＢ７１３には、前述の実施形態とは異なる情報の組み合わせが登録される。次に、図７１（ａ）を参照して、図５５のユーザ情報ＤＢ７１３について詳細に説明する。上述の契約者βは、事業者αからコンテンツ配信を受けるために契約を交わす。この契約に基づいて、事業者αは、契約者βにユーザ識別子Ｉusrを割り当てる。ここで、ユーザ識別子Ｉusrは、契約者βを一意に特定する。さらに、事業者αは、契約者βが管理する機器８１に、前述と同様の機器識別子Ｉdvを割り当てる。なお、上述の実施形態で説明したように、契約者βが、予め機器８１に設定されている機器識別子Ｉdvを事業者αに告知してもよい。機器識別子Ｉdvは、ライセンス情報管理システムＳc1において、契約者βの機器８１を一意に特定する。さらに、事業者αは、契約者βの可搬型記録媒体１０１に記録されているメディア識別子Ｉmdの告知を受ける。以上の機器識別子Ｉdvおよびメディア識別子Ｉmdの組み合わせが、契約者βのために、ユーザ識別子Ｉusrと共に、ユーザ情報ＤＢ７１３に登録される。以上のことから、図７１（ａ）に示すように、ユーザ情報ＤＢ７１３は、ユーザ識別子Ｉusr毎に登録される機器識別子Ｉdvおよびメディア識別子Ｉmdの組み合わせの集まりとなる。

【０２５５】また、前述の実施形態でも説明したように、事業者αにより割り当てられた機器識別子Ｉdvはさらに、契約者β側の機器８１における機器識別子格納部８１１に設定される（図５７参照）。

【０２５６】また、上述の契約者γも、事業者αからコンテンツ配信を受けるために契約を交わす。ここで、説明の便宜のため、契約者γは、契約者βとは異なり、可搬型記録媒体１０１を所有していないとする。以上の契約に基づいて、事業者αは、契約者γに、一意なユーザ

識別子ＩusrＩを割り当てる。さらに、事業者αは、契約者γの機器２０１に、ライセンス情報管理システムＳc1において一意な機器識別子ＩdvIを割り当てる。以上の機器識別子ＩdvIが、契約者γのために、ユーザ情報ＤＢ７１３に、ユーザ識別子ＩusrＩと共に登録される。以上のことから、図７１（ａ）に示すように、ユーザ情報ＤＢ７１３は、ユーザ識別子ＩusrＩ毎に登録される機器識別子ＩdvIの集まりとなる。

【０２５７】また、事業者αにより、機器２０１に割り当てられた機器識別子ＩdvIは、図７０に示すように、契約者γ側の機器２０１における機器識別子格納部８１１に設定される。

【０２５８】なお、以下の説明の便宜のため、図７１（ａ）に示すように、ユーザ情報ＤＢ７１３には、契約者βのために、ユーザ識別子ＩusrＩとしての「ｙ１」に対応して、機器識別子ＩdvIとして「ｘ１」およびメディア識別子ＩmdIとして「ｘ２」が登録されると仮定する。この仮定下では、図５７に示すように、機器８１側の機器識別子格納部８１１には、機器識別子ＩdvIとして「ｘ１」が設定される。さらに、ユーザ情報ＤＢ７１３には、契約者γのために、ユーザ識別子ＩusrＩとしての「ｙ２」に対応して、機器識別子ＩdvIとして「ｘ３」が登録されると仮定する。この仮定下では、図７０に示すように、機器２０１側の機器識別子格納部８１１には、機器識別子ＩdvIとして「ｘ３」が設定される。

【０２５９】ここで、図７１（ｂ）には、利用権データベース７１４が示されているが、当該利用権データベース７１４については、後で説明する。

【０２６０】以上の準備が終了すると、機器８１は、前述の実施形態で説明したように、利用権管理装置７１から、コンテンツデータＤcnt およびライセンス情報Ｄ1cを取得することが可能となる（図６１，図６４～図６６参照）。さらに、本変形例の特徴的な点は、図６８に示すように、契約者βが可搬型記録媒体１０１を契約者γ側に持っていき、当該契約者γ側の機器２０１を使って、コンテンツデータＤcnt およびライセンス情報Ｄ1cの提供を、利用権管理装置７１から受けることができる点である。

【０２６１】以下、図７２および図７３を参照して、契約者βが機器２０１を使ってコンテンツデータＤcnt を取得する際における当該機器２０１および利用権管理装置７１の動作について説明する。まず、契約者βは、契約者γ側の機器２０１に、自分の可搬型記録媒体１０１を装着する。これによって、可搬型記録媒体１０１は、インターフェイス２０２１（図７０参照）を通じて、識別子抽出部２０２２とデータ通信可能に接続される。その後、契約者βは、機器２０１を操作して、利用権管理装置７１にアクセスして、そのコンテンツＤＢ７１１に蓄積されているコンテンツデータＤcnt の中から、今回取得したいもののコンテンツ識別子Ｉcnt を特定する。以降の説明において、今回指定されたコンテンツデータＤcnt を、取得対象コンテンツデータＤcnt と称する。さらに、契約者βは、取得対象コンテンツデータＤcnt を利用する際の利用条件Ｃcnt を指定する。ここで、利用条件Ｃcnt については、前述の実施形態で詳しく説明しているので、ここではその説明を控える。また、本変形例においても、便宜上、利用条件Ｃcnt は、コンテンツデータＤcnt の再生回数であると仮定する。

【０２６２】上述したように、契約者βは、機器２０１を操作して、コンテンツ識別子Ｉcnt および利用条件Ｃcnt を指定する。設定要求生成部８１２（図７０参照）は、契約者βが指定したコンテンツ識別子Ｉcnt および利用条件Ｃcnt を受け取る（ステップＳ４０１）。

【０２６３】次に、設定要求生成部８１２は、識別子抽出部２０２２に、機器識別子ＩdvIおよびメディア識別子ＩmdIのいずれか一方を選択して、自身に返すように指示する。ところで、可搬型記録媒体１０１が機器２０１に装着されている場合、当該機器２０１には、機器識別子格納部８１１に格納されている機器識別子ＩdvIと、可搬型記録媒体１０１に格納されているメディア識別子ＩmdIとが存在することになる。そのため、識別子抽出部２０２２は、設定要求生成部８１２の指示に応答して、可搬型記録媒体１０１が装着されている場合には、インターフェイス２０２１を通じて、当該可搬型記録媒体１０１に格納されているメディア識別子ＩmdIを取り出す。設定要求生成部８１２は、識別子抽出部２０２２により取り出されたメディア識別子ＩmdIを受け取る（ステップＳ４０２）。

【０２６４】ここで、識別子抽出部２０２２は、機器２０１に可搬型記録媒体１０１が装着されていない場合、機器識別子格納部８１１から、機器識別子ＩdvIを取り出して、設定要求生成部８１２に渡すことになる。しかし、この場合、契約者γが、機器２０１を使って、コンテンツデータＤcnt の取得を行うこととなる。このような場合については、本変形例の目的とは関係なく、さらには、識別子抽出部２０２２が機器識別子ＩdvIを取り出す場合における、機器２０１における動作については、前述の実施形態の説明から明らかであるため、その説明を省略する。

【０２６５】設定要求生成部８１２は、以上のメディア識別子ＩmdI、コンテンツ識別子Ｉcnt および利用条件Ｃcnt に、予め保持する設定要求識別子ＩrrIを付加して、設定要求Ｄrr（図７４（ａ）参照）を生成する（ステップＳ４０３）。設定要求Ｄrrは、取得対象コンテンツデータＤcnt の利用権設定を利用権管理装置１１に要求するための情報であるが、本実施形態ではさらに、取得対象コンテンツデータＤcnt の配信を利用権管理装置７１に要求するための情報である。また、設定要求識別子ＩrrIは、利用権管理装置７１が設定要求Ｄrrを特定するために使用される。設定要求生成部８１２は、以上の設定

要求Ｄrrを通信部８１３に渡す。通信部８１３は、受け取った設定要求Ｄrrを、伝送路９１を通じて、利用権管理装置７１に送信する（ステップＳ４０４）。

【０２６６】利用権管理装置７１（図５５参照）において、通信部７１５は、伝送路９１を通じて送信されてくる設定要求Ｄrrを受信して、ユーザ認証部７１６に渡す。ユーザ認証部７１６は、設定要求Ｄrrにユーザ認証処理を行う（ステップＳ４０５）。より具体的には、ユーザ認証部７１６は、上述のユーザ情報ＤＢ７１３（図７１（ａ）参照）を管理しており、受け取った設定要求Ｄrrに設定されているメディア識別子Ｉmdに一致するものが、当該ユーザ情報ＤＢ７１３に登録されているか否かを確認する。ユーザ認証部７１６は、ユーザ情報ＤＢ７１３に一致するものが登録されている場合に限り、今回設定要求Ｄrrが、契約者βからのものであると判断する。さらに、このような判断結果に従って、ユーザ認証部７１６は、ユーザ情報ＤＢ７１３から、今回のメディア識別子Ｉmdに対応するユーザ識別子Ｉusr を取り出して、受け取った設定要求Ｄrrと共に利用権管理部７１７に渡す。

【０２６７】利用権管理部７１７（図５５参照）は、利用権データベース（以下、利用権ＤＢと称する）７１４を管理している。また、利用権管理部７１７は、そこに設定されている設定要求識別子Ｉrrに基づいて、ユーザ認証部７１６から設定要求Ｄrrを渡されれたことを認識する。このような認識結果に従って、利用権管理部７１７は、利用権ＤＢ７１４への利用権登録処理を行う（ステップＳ４０６）。より具体的には、利用権管理部７１７は、設定要求Ｄrrから、コンテンツ識別子Ｉcnt および利用条件Ｃcnt を取り出して、それらと、受け取ったユーザ識別子Ｉusr との組み合わせを利用権ＤＢ７１４に登録する。ここで、利用権管理部７１７は、設定要求Ｄrrに設定されている利用条件Ｃcnt で、契約者βが取得対象コンテンツデータＤcnt を利用する権利の設定を要求しているとみなす。つまり、利用権管理部７１７からみれば、利用条件Ｃcnt は、取得対象コンテンツデータＤcnt を契約者βが利用できる権利を示す。以上の観点から、利用権管理部７１７は、設定要求Ｄrrから取り出した利用条件Ｃcnt を利用権情報Ｄrqt として扱う。つまり、利用権ＤＢ７１４は、図７１（ｂ）に示すように、ユーザ識別子Ｉusr 、コンテンツ識別子Ｉcnt および利用権情報Ｄrqt の組み合わせの集まりとなる。これによって、利用権管理部７１７は、契約者βの取得対象コンテンツデータＤcnt の利用権を管理する。利用権管理部７１７は、以上の利用条件登録処理が終了すると、今回受け取った設定要求Ｄrrをコンテンツ管理部７１８に渡す。

【０２６８】ここで、以上の利用権ＤＢ７１４に登録される利用権情報Ｄrqt の具体例について登録する。既に説明している通り、本実施形態では、利用条件Ｃcnt は利用回数であると仮定されている。さらに、今回の設定要求Ｄrrには、メディア識別子Ｉmdとして「ｘ１」、コンテンツ識別子Ｉcnt として「ａ」および利用条件Ｃcnt として「再生m回」（mは自然数）が設定されていると仮定する。以上の仮定下では、ユーザ認証部７１６は、ステップＳ４０５のユーザ認証処理において、ユーザ識別子Ｉusr としての「ｙ１」を、ユーザ情報ＤＢ７１３から取り出して、利用権管理部７１７に渡す。従って、ステップＳ４０６では、図７１（ｂ）に示すように、１つの利用条件情報Ｄcrt には、ユーザ識別子Ｉusr としての「ｙ１」、コンテンツ識別子Ｉcnt としての「ａ」および利用権情報Ｄrqt としての「再生m回」が設定される。

【０２６９】なお、本ライセンス情報管理システムＳc1の技術的特徴とは関係ないが、ステップＳ４０６において、利用権管理部７１７は、利用条件情報Ｄcrt の登録毎に、ユーザ識別子Ｉusr が割り当てられている契約者βに対して課金を行ってもよい。

【０２７０】コンテンツ管理部７１８は、設定要求Ｄrrを受け取ると、図６１のステップＳ２０４と同様の読み出し処理を行う（ステップＳ４０７）。その後、コンテンツ暗号化部７１９は、ステップＳ２０５と同様の暗号処理を行う（ステップＳ４０８）。さらに、送信データ生成部７２０は、ステップＳ２０６と同様の送信データ生成処理を行う（ステップＳ４０９）。その結果、ステップＳ２０６と同様に、送信データＤtrm （図６２（ｂ）参照）が、伝送路９１を介して、機器２０１へと送信される（ステップＳ４０１０）。

【０２７１】機器２０１（図７０参照）において、通信部８１３は、図６１のステップＳ２０８と同様の受信処理を行う（図７３：ステップＳ４０１１）。コンテンツ管理部８１４は、ステップＳ２０９と同様の蓄積処理を行う（ステップＳ４０１２）。その結果、コンテンツ蓄積部８１５には、図６３を参照して説明したように、コンテンツ識別子Ｉcnt および暗号済みコンテンツデータＤecntの組み合わせが、いくつか蓄積されることになる。

【０２７２】前述の実施形態での説明と同様に、機器２０１には暗号済みコンテンツデータＤecntが配信される。そのため、機器２０１は、コンテンツデータＤcnt を利用する場合には、利用権管理装置７１により提供される復号鍵Ｋd で、暗号済みコンテンツデータＤecntを復号する必要がある。ここで、本ライセンス情報管理システムＳc1では、復号鍵Ｋd を、契約者βが操作中の機器２０１に提供するために、後で詳説するライセンス情報Ｄlcが用いられる。以下、図７５～図７７を参照して、ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器２０１および利用権管理装置７１の動作について説明する。

【０２７３】まず、契約者βは、機器２０１を操作し

て、コンテンツ蓄積部８１５にアクセスして、そこに蓄積されている暗号済みコンテンツデータＤecntの中から、今回利用したいものを特定する。ここで、以下の説明において、今回指定された暗号済みコンテンツデータＤecntを、復号対象コンテンツデータＤecntと称する。

【０２７４】コンテンツ管理部８１４（図７０参照）は、コンテンツ蓄積部８１５を管理しており、契約者βにより特定された復号対象コンテンツデータＤecntに付加されているコンテンツ識別子Ｉcnt を、当該コンテンツ蓄積部８１５から取り出す。発行要求生成部８１６は、コンテンツ管理部８１４により取り出されたコンテンツ識別子Ｉcnt を受け取る（ステップＳ５０１）。

【０２７５】次に、発行要求生成部８１６は、識別子抽出部２０２２に、機器識別子Ｉdvおよびメディア識別子Ｉmdのいずれか一方を選択して、自身に返すように指示する。識別子抽出部２０２２は、発行要求生成部８１６の指示に応答して、可搬型記録媒体１０１が装着されている場合には、インターフェイス２０２１を通じて、当該可搬型記録媒体１０１に格納されているメディア識別子Ｉmdを取り出す。発行要求生成部８１６は、識別子抽出部２０２２により取り出されたメディア識別子Ｉmdを受け取る（ステップＳ５０２）。

【０２７６】ここで、識別子抽出部２０２２は、前述したように、機器２０１に可搬型記録媒体１０１が装着されていない場合、機器識別子格納部８１１から、機器識別子Ｉdvを取り出して、設定要求生成部８１２に渡す。しかし、この場合、契約者γが、機器２０１を使って、ライセンス情報Ｄlcの提供を受けることとなる。このような場合については、本変形例の目的とは関係なく、さらには、識別子抽出部２０２２が機器識別子Ｉdvを取り出す場合における、機器２０１における動作については、前述の実施形態の説明から明らかであるため、その説明を省略する。

【０２７７】その後、発行要求生成部８１６は、メディア識別子Ｉmdおよびコンテンツ識別子Ｉcnt に、発行要求識別子Ｉirを付加して、発行要求Ｄir（図７４（ｂ）参照）を生成する（ステップＳ５０３）。ここで、発行要求Ｄirは、上述のライセンス情報Ｄlcの提供を利用権管理装置７１に要求するための情報である。また、発行要求識別子Ｉirは、利用権管理装置７１が発行要求Ｄir を特定するために使用される。発行要求生成部８１６は、以上の発行要求Ｄirを通信部８１３に渡す。通信部８１３は、受け取った発行要求Ｄirを伝送路９１を通じて、利用権管理装置７１に送信する（ステップＳ５０４）。

【０２７８】利用権管理装置７１において、通信部７１５（図５５参照）は、伝送路９１を通じて送信されてくる発行要求Ｄirを受信して、ユーザ認証部７１６に渡す。ユーザ認証部７１６は、発行要求Ｄirを受け取ると、ユーザ認証部７１６は、発行要求Ｄirにユーザ認証処理を行う（ステップＳ５０５）。より具体的には、ユーザ認証部７１６は、受け取った発行要求Ｄirに設定されているメディア識別子Ｉmdに一致するものが、ユーザ情報ＤＢ７１３（図７１（ａ）参照）に登録されているか否かを確認する。ユーザ認証部７１６は、ユーザ情報ＤＢ７１３に一致するものが登録されている場合に限り、今回の発行要求Ｄirが、契約者βからのものであると判断する。さらに、このような判断結果に従って、ユーザ認証部７１６は、ユーザ情報ＤＢ７１３から、今回のメディア識別子Ｉmdに対応するユーザ識別子Ｉusr を取り出して、受け取った発行要求Ｄirと共に利用権管理部７１７に渡す。

【０２７９】利用権管理部７１７は、発行要求Ｄirに設定されている発行要求識別子Ｉirに基づいて、今回、ユーザ認証部７１６から発行要求Ｄirを渡されたことを認識する。このような認識結果に従って、利用権管理部７１７は、受け取った発行要求Ｄirからコンテンツ識別子Ｉcnt を取り出す（ステップＳ５０６）。次に、利用権管理部７１７は、受け取ったユーザ識別子Ｉusr および取り出したコンテンツ識別子Ｉcnt の組み合わせが、利用権ＤＢ７１４（図７１（ｂ）参照）に登録されているか否かを判断する（ステップＳ５０７）。

【０２８０】利用権管理部７１７は、ステップＳ５０７で「Ｙｅｓ」と判断した場合、それらと同じ組みの利用権情報Ｄrqt を参照して、契約者βが操作中の機器２０１に利用許可を与えることができるか否かを判断する（ステップＳ５０８）。ステップＳ５０８で「Ｙｅｓ」と判断した場合、利用権管理部７１７は、利用権情報Ｄrqt の一部または全てを取り出す（ステップＳ５０９）。ここで、以下の説明において混同が生じることを避けるため、ステップＳ５０９において取り出された一部または全ての利用権情報Ｄrqt のことを、今回の発行要求Ｄirにより特定される契約者βの機器２０１にコンテンツデータＤcnt の利用を許可するための情報であるという観点から、利用許可情報Ｄlwと称する。つまり、ステップＳ５０９では、利用許可情報Ｄlwが生成される。

【０２８１】利用許可情報Ｄlwの生成により、契約者βのために登録されている利用権情報Ｄrqt の一部または全てが使用される。そのため、ステップＳ５０９の次に、利用権管理部７１７は、ステップＳ５０９で一部または全部が取り出された利用権情報Ｄrqt を更新する（図７５；ステップＳ５０１０）。

【０２８２】ここで、以上のステップＳ５０６～Ｓ５０１０の処理の具体例について登録する。今、利用権ＤＢ７１４には、図７１（ｂ）に示すように、ユーザ識別子Ｉusr としての「ｙ１」、コンテンツ識別子Ｉcnt としての「ａ」および利用権情報Ｄrqt としての「再生m回」の組みが登録されていると仮定する。また、今回、機器２０１は、メディア識別子Ｉmdとしての「ｘ２」お

よびコンテンツ識別子Ｉcnt としての「ａ」が設定されている発行要求Ｄirを送信すると仮定する。

【０２８３】以上の仮定下では、ステップＳ５０６において、利用権管理部７１７は、ユーザ識別子Ｉusr としての「ｙ１」を受け取り、さらに、発行要求Ｄirから、コンテンツ識別子Ｉcnt としての「ａ」を取り出す。また、ステップＳ５０７において、ユーザ識別子Ｉusr としての「ｙ１」およびコンテンツ識別子Ｉcnt としての「ａ」の組みが、利用権ＤＢ７１４に登録されていると判断される。このように判断されると、ステップＳ５０８において、同じ組みの利用権情報Ｄrqt には、「再生m回」と設定されているので、契約者βが操作中の機器２０１の利用許可を与えてもよいと判断される。このように判断されると、ステップＳ５０９において、利用許可情報Ｄ１wが生成される。この時生成される利用許可情報Ｄ１wとしては、例えば、「再生ｎ回」が挙げられる。ここで、ｎは、上述のmを超えない自然数であり、より好ましくは、機器２０１の処理能力に応じて設定される。例えば、機器２０１が相対的に低い性能のハードウェアを搭載している場合であれば、ｎは、「１」のように、機器２０１が復号対象コンテンツデータＤecntを利用可能な最低限の値に設定されることが好ましい。

【０２８４】以上のステップＳ５０６～Ｓ５０９により、機器２０１に装着された可搬型記録媒体１０１（メディア識別子Ｉmdが「ｘ２」）がコンテンツデータＤcnt（コンテンツ識別子Ｉcnt「ａ」）を再生する権利をｎ回使うことになる。そのため、ステップＳ５０１０において、契約者βの利用権情報Ｄrqt が「再生m回」から「再生（m－ｎ）回」に更新される。

【０２８５】以上のようにして生成した利用許可情報Ｄ１wを、利用権管理部７１７（図５５参照）は、発行要求Ｄirと一緒に、ライセンス情報生成部７２１に渡す。より具体的には、ライセンス情報生成部７２１は、図５６に示すように、ハッシュ値生成部７２１１およびライセンス情報組立部７２１２を含んでいる。ハッシュ値生成部７２１１には、利用許可情報Ｄ１wのみが渡され、また、ライセンス情報組立部７２１２には、利用許可情報Ｄ１wおよび発行要求Ｄirの双方が渡される。

【０２８６】まず、ハッシュ値生成部７２１１は、図６４のステップＳ３０８と同様にして、ハッシュ値Ｖhsを生成し（ステップＳ５０１１）、生成したハッシュ値Ｖhsをライセンス情報組立部７２１２に渡す。ライセンス情報組立部７２１２は、受け取った発行要求Ｄirを復号鍵管理部７２２に渡す。復号鍵管理部７２２（図５５参照）は、前述した復号鍵ＤＢ７１２（図５９（ｂ）参照）を管理する。復号鍵管理部７２２は、受け取った発行要求Ｄirに設定されているコンテンツ識別子Ｉcnt およびメディア識別子Ｉmdを取り出す。さらに、復号鍵管理部７２２は、コンテンツ識別子Ｉcnt と同じ組みの復号鍵Ｋd を復号鍵ＤＢ７１２から取り出して、メディア識別子Ｉmdと一緒に復号鍵暗号化部７２３に渡す。復号鍵暗号化部７２３は、受け取った復号鍵Ｋd を、同時に受け取ったメディア識別子Ｉmdで暗号化して（ステップＳ５０１２）、暗号済みの復号鍵Ｋedを生成する。以上の暗号済み復号鍵Ｋedは、ライセンス情報組立部７２１２に渡される。

【０２８７】ライセンス情報組立部７２１２は、発行要求Ｄirおよび利用許可情報Ｄ１w、ハッシュ値Ｖhsならびに暗号済み復号鍵Ｋedのすべてが揃うと、図６５のステップＳ３０１０と同様にして、図６７（ｂ）に示すライセンス情報Ｄ１cを生成する（ステップＳ５０１３）。以上のライセンス情報Ｄ１cは、通信部７１５に渡される。通信部７１５から、伝送路９１を通じて、機器２０１に送信される（ステップＳ５０１４）。

【０２８８】機器２０１（図７０参照）において、通信部８１３は、ステップＳ３０１２と同様にして、伝送路９１を通じて送信されてくるライセンス情報Ｄ１cを受信し（ステップＳ５０１５）、ライセンス情報処理部８１７に渡す。

【０２８９】ライセンス情報処理部８１７は、図５８に示すように、改竄判定部８１７１と、ハッシュ値生成部８１７２と、利用許可判定部８１７３と、復号鍵復号部８１７４とを含んでいる。通信部８１３からのライセンス情報Ｄ１cは、まず、改竄判定部８１７１に渡される。改竄判定部８１７１は、まず、ステップＳ３０１３と同様に、受け取ったライセンス情報Ｄ１cから、利用許可情報Ｄ１wを取り出し、さらに、ハッシュ値Ｖhsを外部ハッシュ値Ｖehs として取り出し（ステップＳ５０１６）、取り出した利用許可情報Ｄ１wを、ハッシュ値生成部８１７２に渡し、外部ハッシュ値Ｖehs をそのまま保持する。

【０２９０】ハッシュ値生成部８１７２は、ステップＳ３０１４と同様にして、内部ハッシュ値Ｖ１hs を生成して（ステップＳ５０１７）、改竄判定部８１７１に返す。

【０２９１】改竄判定部８１７１は、上述の内部ハッシュ値Ｖ１hs を受け取ると、ステップＳ３０１５と同様にして、利用許可情報Ｄ１wが改竄されているか否かを判定し（ステップＳ５０１８）、「Ｙｅｓ」と判定した場合には、今回受け取ったライセンス情報Ｄ１cを利用許可判定部８１７３に渡す。

【０２９２】利用許可判定部８１７３は、受け取ったライセンス情報Ｄ１cを参照して、ステップＳ３０１６と同様にして、復号対象コンテンツデータＤecntの利用が許可されているか否かを判定する（ステップＳ５０１９）。利用許可判定部８１７３は、ステップＳ５０１９において「Ｙｅｓ」と判断した場合に限り、受け取ったライセンス情報Ｄ１cから、暗号済み復号鍵Ｋedを取り出して、復号鍵復号部８１７４に渡す。

【０２９３】ここで、以上のステップＳ５０１９の処理

の具体例について説明する。前述の仮定に従えば、今回のライセンス情報Ｄｌｃの利用許可情報Ｄｌｗにより、コンテンツデータＤｃｎｔ の再生がｎ回だけ許可されている。かかる場合、利用許可判定部８１７３は、ステップＳ５０１９において、利用許可情報Ｄｌｗに設定される再生回数が１以上であれば、復号対象コンテンツデータＤｅｃｎｔの利用が許可されていると判断して、受け取ったライセンス情報Ｄｌｃから暗号済み復号鍵Ｋｅｄを取り出して、復号鍵復号部８１７４に渡す。

【０２９４】さて、復号鍵復号部８１７４は、利用許可判定部８１７３から暗号済み復号鍵Ｋｅｄを受け取る。さらに、復号鍵復号部８１７４は、識別子抽出部２０２２に、機器識別子Ｉｄｖおよびメディア識別子Ｉｍｄのいずれか一方を選択して、自身に返すように指示する。識別子抽出部２０２２は、復号鍵復号部８１７４の指示に応答して、可搬型記録媒体１０１が装着されている場合には、インターフェイス２０２１を通じて、当該可搬型記録媒体１０１に格納されているメディア識別子Ｉｍｄを取り出す。復号鍵復号部８１７４は、識別子抽出部２０２２により取り出されたメディア識別子Ｉｍｄを受け取る。

【０２９５】ここで、識別子抽出部２０２２は、機器２０１に可搬型記録媒体１０１が装着されていない場合、機器識別子格納部８１１から、機器識別子Ｉｄｖを取り出して、復号鍵復号部８１７４に渡すことになる。このような場合については、本変形例の目的とは関係なく、さらには、識別子抽出部２０２２が機器識別子Ｉｄｖを取り出す場合における、機器２０１における動作については、前述の実施形態と同様であるため、その説明を省略する。

【０２９６】以上のようにして、メディア識別子Ｉｍｄを受け取ると、復号鍵復号部８１７４は、暗号済み復号鍵Ｋｅｄを、メディア識別子Ｉｍｄで復号して（図７７：ステップＳ５０２０）、復号鍵Ｋｄ をコンテンツ復号部８１８に渡す。

【０２９７】ところで、コンテンツ管理部８１４は、ステップＳ５０１において、コンテンツ識別子Ｉｃｎｔ だけでなく、前述の復号対象コンテンツデータＤｅｃｎｔを取り出す。取り出された復号対象コンテンツデータＤｅｃｎｔは、コンテンツ復号部８１８に渡される。コンテンツ復号部８１８は、復号鍵復号部８１７４から受け取った復号鍵Ｋｄ で、復号対象コンテンツデータＤｅｃｎｔを復号して（ステップＳ５０２１）、コンテンツデータＤｃｎｔ をコンテンツ再生部８１９に渡す。コンテンツ再生部８１９は、受け取ったコンテンツデータＤｃｎｔ を再生して、音声出力する（ステップＳ５０２２）。これにより、契約者βは、事業者αから購入したコンテンツデータＤｃｎｔ が表す音楽を聴くことができる。以上説明したように、本ライセンス情報管理システムＳｃ1によれば、契約者βは、自分が得た利用権情報Ｄｒｑｔを使って、別の契約者γが管理する機器２０１で、コンテンツデータＤｃｎｔ を利用することが可能となる。これによって、より使い勝手のよいライセンス情報管理システムＳｃ1を提供することが可能となる。

【０２９８】ここで、図７６のステップＳ５０１８において、改竄判定部８１７１は、利用許可情報Ｄｌｗが改竄されていると判定する場合がある。また、ステップＳ５０１９において、利用許可判定部８１７３は、復号対象コンテンツデータＤｅｃｎｔの利用が許可されていないと判定する場合もある。このような場合、改竄判定部８１７１および利用許可判定部８１７３は、図６６のステップＳ３０２０を実行して、今回受け取ったライセンス情報Ｄｌｃを破棄する。

【０２９９】また、図７５のステップＳ５０７において、利用権管理部７１７は、ユーザ識別子Ｉｕｓｒ およびコンテンツ識別子Ｉｃｎｔ の組み合わせが、利用権ＤＢ７１４（図７１（ｂ）参照）に登録されていないと判断する場合がある。さらに、ステップＳ５０８において、利用権管理部７１７は、契約者βが操作中の機器２０１に利用許可を与えないと判断する場合もある。このような場合、利用権管理部７１７は、図６６のステップＳ３０２１を実行して、利用拒否情報Ｄｒｊを生成して、通信部７１５に渡す。通信部７１５は、受け取った利用拒否情報Ｄｒｊを、伝送路９１を介して、機器２０１に送信する。これによって、前述の実施形態と同様に、機器２０１が、復号対象コンテンツデータＤｅｃｎｔを復号しないようにすることができる。

【０３００】なお、ステップＳ５０７において、利用権管理部７１７は、ユーザ識別子Ｉｕｓｒ.およびコンテンツ識別子Ｉｃｎｔ の組み合わせが、利用権ＤＢ７１４（図７１（ｂ）参照）に登録されていないと判断する場合に、ユーザ識別子Ｉｕｓｒ 、コンテンツ識別子Ｉｃｎｔ および利用権情報Ｄｒｑｔ を生成して、利用権ＤＢ７１４に登録するようにしてもよい。

【０３０１】なお、以上の変形例において、契約者β側には、前述の実施形態で説明した機器８１が設置されるとして説明したが、これに限らず、上述の機器２０１が設置されてもよい。

【０３０２】また、以上の変形例において、機器２０１は、機器識別子格納部８１１を備えるとして説明した。しかしながら、契約者γ自身が機器２０１を使ってコンテンツデータＤｃｎｔ およびライセンス情報Ｄｌｃの提供を利用権管理装置７１から受けない場合には、機器２０１は、機器識別子格納部８１１を備える必要性はない。

【０３０３】また、以上の変形例においても、前述の実施形態と同様に、互いに異なる利用権管理装置が図７２および図７３の処理と図７５～図７７の処理とを行うようにしてもよい。さらに、本変形例においても、最初にライセンス情報Ｄｌｃの取得が行われ、その後に、コンテンツデータＤｃｎｔ の取得が行われても良い。また、コンテンツデータＤｃｎｔ の取得およびライセンス情報Ｄｌｃの

取得が同時並行して行われてもよい。

【０３０４】また、以上の変形例では、説明の便宜上、ユーザ情報ＤＢ７１３には、ユーザ識別子Ｉusr と、機器識別子Ｉdvおよび／またはメディア識別子Ｉmdが登録されるとして説明した。しかしながら、前述の実施形態と同様に、ユーザ情報ＤＢ７１３にはさらに、契約者βを一意に特定可能な他のユーザ情報（例えば、住所および電話番号）が登録されてもよい。

【０３０５】また、以上の変形例は、前述の実施形態と同様、機器２０１におけるコンテンツ再生部８１９は、コンテンツデータＤcnt の種類に応じて、テレビ番組、映画、書籍および印刷物およびゲーム内容を映像出力可能なもの、ラジオ番組を音声出力可能なものに置換されてもよい。さらに、機器２０１は、以上のようなコンテンツ再生部８１９に代えて、復号されたコンテンツデータＤcnt を、外部の機器（テレビジョン受像機、ラジオ受信機、音楽再生機、電子ブックリーダ、ゲーム機器、ＰＣ、情報携帯端末、携帯電話、外部記憶装置等）に転送可能なインターフェイスを備えていてもよい。

【０３０６】また、以上の変形例においても、前述の実施形態と同様、ＳＳＬ等の保護技術を適用するという条件で、ライセンス情報Ｄ1cは、暗号化されていない復号鍵Ｋｄをそのまま含んでいてもよい。また、デジタルライツを保護するために、機器２０１には、可搬型記録媒体１０１に格納されるメディア識別子Ｉmdでライセンス情報Ｄ1cを暗号化するアルゴリズムが組み込まれることがより好ましい。

【０３０７】また、以上の第６の変型例に係るインターフェイス２０２１および識別子抽出部２０２２は、第２の実施形態に係る機器５１に組み込まれても良い。このように、機器５１ａまたは５１ｂに、インターフェイス２０２１および識別子抽出部２０２２の両者を組み込んだ場合、識別子抽出部２０２２は、ユーザの指定に従って、機器５１ａまたは５１ｂの機器識別子格納部２１１に設定されている機器識別子Ｉdva またはＩdvb もしくは、可搬型記録媒体１０１に格納されているメディア識別子Ｉmdのいずれかを使って、設定要求Ｄrrを生成して、利用権管理装置４１に送信する。これによって、ユーザは、機器５１ａまたは５１ｂもしくは可搬型記録媒体１０１のいずれかを使って、コンテンツデータＤcnt を利用できるようになるので、より使い勝手の良いライセンス情報管理システムＳb を実現できるようになる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る利用権管理装置１１を収容したライセンス情報管理システムＳａの全体構成を示すブロック図である。

【図２】図１の利用権管理装置１１の詳細な構成を示すブロック図である。

【図３】図２のライセンス情報生成部１２１の詳細な構成を示すブロック図である。

【図４】図１の機器２１ａおよび２１ｂの詳細な構成を示すブロック図である。

【図５】図４のライセンス情報処理部２１７の詳細な構成を示すブロック図である。

【図６】図２のコンテンツＤＢ１１１および図２の復号鍵ＤＢ１１２を示す模式図である。

【図７】図２のユーザ情報ＤＢ１１３および図２の利用権ＤＢ１１４を示す模式図である。

【図８】コンテンツデータＤcnt の利用権設定および取得時における、機器２１ａおよび利用権管理装置１１の動作を示すフローチャートである。

【図９】図８に示す処理の過程で送受される設定要求Ｄrrおよび送信データＤtrn のフォーマットを示す模式図である。

【図１０】図４のコンテンツ蓄積部２１５に蓄積されるデータを示す模式図である。

【図１１】ライセンス情報Ｄ1ca の取得およびコンテンツデータＤcnt の復号時における機器２１ａおよび利用権管理装置１１の動作を示す第１のフローチャートである。

【図１２】ライセンス情報Ｄ1ca の取得およびコンテンツデータＤcnt の復号時における機器２１ａおよび利用権管理装置１１の動作を示す第２のフローチャートである。

【図１３】ライセンス情報Ｄ1ca の取得およびコンテンツデータＤcnt の復号時における機器２１ａおよび利用権管理装置１１の動作を示す第３のフローチャートである。

【図１４】図１２～図１３の処理の過程で送受される発行要求Ｄir、ライセンス情報Ｄ1cおよび利用拒否情報Ｄrjのフォーマットを示す模式図である。

【図１５】図１の利用権管理装置１１の第１の変型例に係る利用権管理装置１１ａを収容したライセンス情報管理システムＳa1の全体構成を示すブロック図である。

【図１６】図１５に示す利用権管理装置１１ａの詳細な構成を示すブロック図である。

【図１７】図１５に示す機器２１ｃの詳細な構成を示すブロック図である。

【図１８】図１５の機器２１ｃをユーザ情報ＤＢ１１３に登録するまでの機器２１ｃおよび利用権管理装置１１ａの動作を示すフローチャートである。

【図１９】図１８の処理の過程で送受される登録要求Ｄrsc 、登録完了通知Ｄscc および登録拒否通知Ｄsrc のフォーマットを示す模式図である。

【図２０】図１８の処理により更新されたユーザ情報ＤＢ１１３を示す模式図である。

【図２１】図１の利用権管理装置１１の第２の変型例に係る利用権管理装置１１ｂの詳細な構成を示すブロック図である。

【図２２】第２の変型例に係る機器２１ａまたは２１ｂ

の詳細な構成を示すブロック図である。
【図２３】第２の変型例に係る機器２１ｃの詳細な構成を示すブロック図である。
【図２４】機器２１ｃの機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録する際における機器２１ａおよび利用権管理装置１１ｂの動作を示すフローチャートである。
【図２５】機器２１ｃの機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録する際における機器２１ｃおよび利用権管理装置１１ｂの動作を示すフローチャートである。
【図２６】図２４の処理の過程で送受される仮登録要求Ｄprscおよび仮登録完了通知Ｄpsccのフォーマットを示す模式図である。
【図２７】図２４および図２５の処理により更新されたユーザ情報ＤＢ１１３を示す模式図である。
【図２８】図２５の処理の過程で送受される本登録要求Ｄcrscおよび本登録完了通知Ｄcsccのフォーマットを示す模式図である。
【図２９】図１の利用権管理装置１１の第３の変型例に係る利用権管理装置１１ｃの詳細な構成を示すブロック図である。
【図３０】第３の変型例に係る機器２１ａまたは２１ｂの詳細な構成を示すブロック図である。
【図３１】第３の変型例に係る機器２１ｃの詳細な構成を示すブロック図である。
【図３２】機器２１ｃの機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録する際における、機器２１ｃおよび利用権管理装置１１ｃの動作を示すフローチャートである。
【図３３】機器２１ｃの機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録する際における、機器２１ａおよび利用権管理装置１１ｃの動作を示すフローチャートである。
【図３４】図３２の処理の過程で送受されるパスワード要求Ｄrps およびパスワード通知Ｄpss のフォーマットを示す模式図である。
【図３５】図３２および図３３の処理により更新されたユーザ情報ＤＢ１１３を示す模式図である。
【図３６】図３３の処理の過程で送受される登録要求Ｄrsc およびび登録完了通知Ｄscc のフォーマットを示す模式図である。
【図３７】図１の利用権管理装置１１の第４の変型例に係る利用権管理装置１１ｄの詳細な構成を示すブロック図である。
【図３８】第４の変型例に係る機器２１ａまたは２１ｂの詳細な構成を示すブロック図である。
【図３９】第４の変型例に係る機器２１ｃの詳細な構成を示すブロック図である。
【図４０】機器２１ｃの機器識別子Ｉdvc をユーザ情報ＤＢ１１３に登録するまでの機器２１ａ、機器２１ｃおよび利用権管理装置１１ｄの動作を示すフローチャートである。
【図４１】図４０の処理の過程で送受される第１の登録要求Ｄrsc1 、第２の登録要求Ｄrsc およびび登録完了通知Ｄscc のフォーマットを示す図である。
【図４２】図１の利用権管理装置１１の第５の変型例に係る利用権管理装置１１ｅを収容したライセンス情報管理システムＳa5の全体構成を示すブロック図である。
【図４３】図４２に示す利用権管理装置１１ｅの詳細な構成を示すブロック図である。
【図４４】図４２に示す機器２１ｂの詳細な構成を示すブロック図である。
【図４５】機器２１ｂの機器識別子Ｉdvb をユーザ情報ＤＢ１１３および利用権ＤＢ１１４から削除するまでの機器２１ｂおよび利用権管理装置１１ｅの動作を示すフローチャートである。
【図４６】図４５の処理の過程で送受される削除要求Ｄrwb およびび削除完了通知Ｄswb のフォーマットを示す模式図である。
【図４７】図４５の処理により更新されたユーザ情報ＤＢ１１３を示す模式図である。
【図４８】本発明の第２の実施形態に係る利用権管理装置４１を収容したライセンス情報管理システムＳb の全体構成を示すブロック図である。
【図４９】図４８の利用権管理装置４１の詳細な構成を示すブロック図である。
【図５０】図４８の機器５１ａおよび５１ｂの詳細な構成を示すブロック図である。
【図５１】コンテンツデータＤcnt の取得時における機器５１ａおよび利用権管理装置４１の動作を示すフローチャートである。
【図５２】図４９の利用権ＤＢ１１４を示す模式図である。
【図５３】図５１の処理の過程で送受される第２の設定要求Ｄrr2bのフォーマットを示す図である。
【図５４】本発明の第３の実施形態に係るライセンス情報管理システムＳc の全体構成を示すブロック図である。
【図５５】図５４の利用権管理装置７１の詳細な構成を示す機能ブロック図である。
【図５６】図５５のライセンス情報生成部７２１の詳細な構成を示す図である。
【図５７】図５４の機器８１の詳細な構成を示す機能ブロック図である。
【図５８】図５７のライセンス情報処理部８１７の詳細な構成を示す機能ブロック図である。
【図５９】図５５のコンテンツＤＢ７１１および図５５の復号鍵ＤＢ７１２を示す模式図である。
【図６０】図５５のユーザ情報ＤＢ７１３および利用権ＤＢ７１４を示す模式図である。
【図６１】コンテンツデータＤcnt の取得時における機

器８１および利用権管理装置７１の動作を示すフローチャートである。

【図６２】図６１の処理の過程で送受される設定要求Ｄrrおよび送信データＤtrn のフォーマットを示す模式図である。

【図６３】図５８のコンテンツ蓄積部８１５に格納されるデータを示す模式図である。

【図６４】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器８１および利用権管理装置７１の動作を示す第１のフローチャートである。

【図６５】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器８１および利用権管理装置７１の動作を示す第２のフローチャートである。

【図６６】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器８１および利用権管理装置７１の動作を示す第３のフローチャートである。

【図６７】図６４～図６６の処理の過程で送受される発行要求Ｄir、ライセンス情報Ｄlcおよび利用拒否情報Ｄrjのフォーマットを示す模式図である。

【図６８】図５４のライセンス情報管理システムＳｃの変型例に係るライセンス情報管理システムＳc1の全体構成を示すブロック図である。

【図６９】図６８の可搬型記録媒体１０１の構成を示す模式図である。

【図７０】図６８の機器２０１の詳細な構成を示す機能ブロック図である。

【図７１】図６８のユーザ情報ＤＢ７１３および利用権ＤＢ７１４を示す模式図である。

【図７２】契約者βが機器２０１を使ってコンテンツデータＤcnt を取得する際における当該機器２０１および利用権管理装置７１の動作を示す第１のフローチャートである。

【図７３】契約者βが機器２０１を使ってコンテンツデータＤcnt を取得する際における当該機器２０１および利用権管理装置７１の動作を示す第２のフローチャートである。

【図７４】図７２および図７３の処理の過程で送受される設定要求Ｄrrおよび発行要求Ｄirのフォーマットを示す模式図である。

【図７５】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器２０１および利用権管理装置７１の動作を示す第１のフローチャートである。

【図７６】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器２０１および利用権管理装置７１の動作を示す第２のフローチャートである。

【図７７】ライセンス情報Ｄlcの取得およびコンテンツデータＤcnt の復号時における機器２０１および利用権管理装置７１の動作を示す第３のフローチャートである。

【符号の説明】

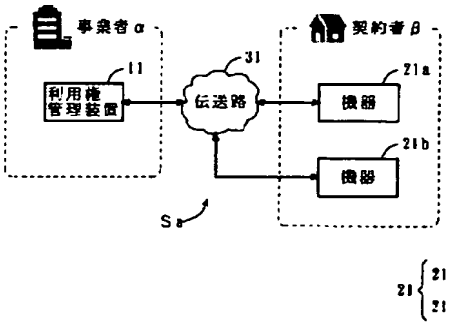
Ｓa，Ｓa1～Ｓa5，Ｓb，Ｓc，Ｓc1…ライセンス情報管理システム

１１，１１a～１１e，４１，７１…利用権管理装置

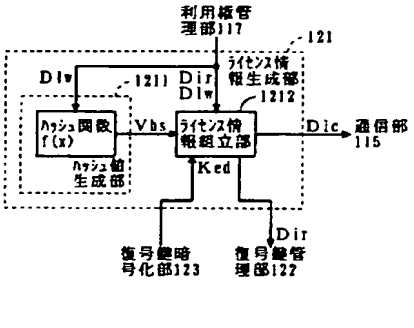
２１a～２１c，５１a，５１b，８１，２０１…機器

１０１…可搬型記録媒体

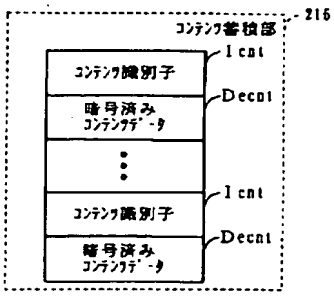
【図１】



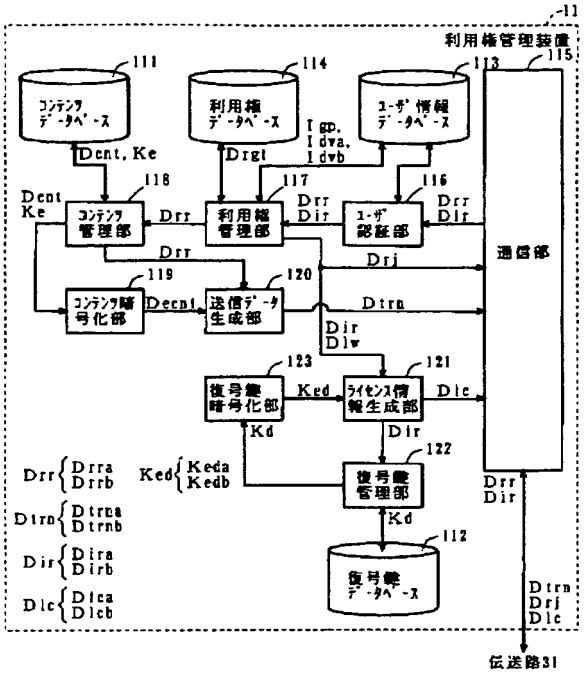
【図３】



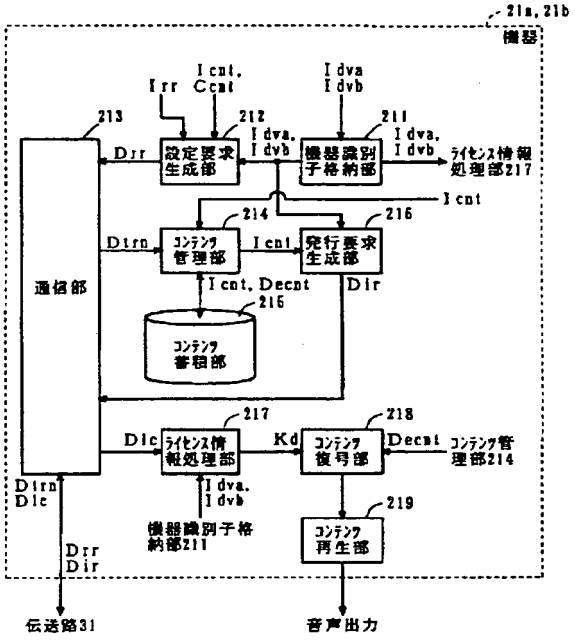
【図１０】



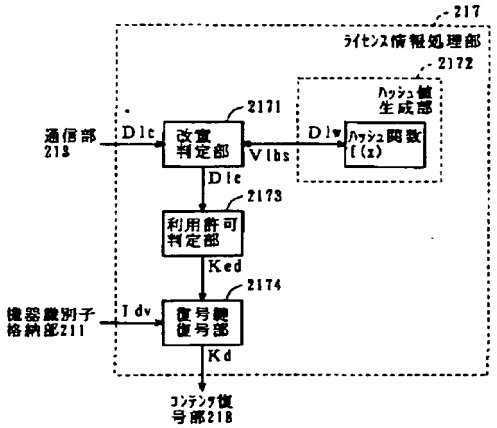
【図２】


11
利用権管理装置
111
コンテンツデータベース
114
利用権データベース
113
ユーザ情報データベース
115
通信部
Dcnt, Ke
Drgt
Igp, Idva, Idvb
118
コンテンツ管理部
117
利用権管理部
116
ユーザ認証部
Dcnt Ke
Drr
Drr Dir
Drj
119
コンテンツ暗号化部
Decnt
120
送信データ生成部
Dtrn
Dir Dlw
123
復号鍵暗号化部
Ked
121
ライセンス情報生成部
Dlc
Kd
Dir
122
復号鍵管理部
Drr { Drra Drrb
Ked { Keda Kedb
Dtrn { Dtrna Dtrnb
Dir { Dira Dirb
Dlc { Dlca Dlcb
Kd
112
復号鍵データベース
Drr Dir
Dtrn Drj Dlc
伝送路31

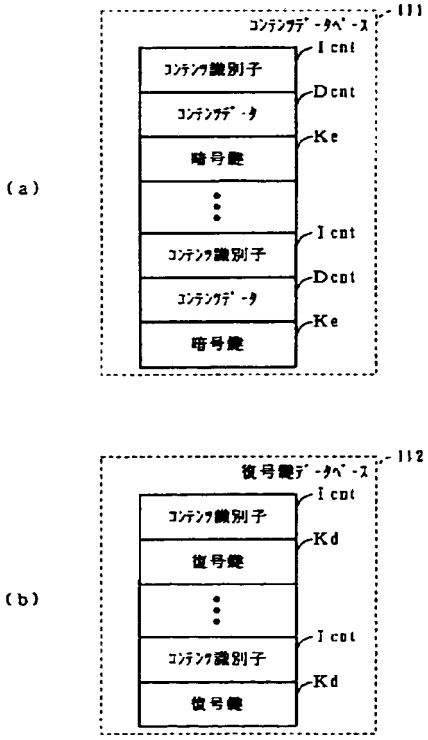
【図４】


21a, 21b
機器
Icnt, Irr Ccnt
Idva Idvb
213
212
211
Drr
設定要求生成部
Idva, Idvb
機器識別子格納部
ライセンス情報処理部217
Icnt
214
216
Dtrn
コンテンツ管理部
Icnt
発行要求生成部
通信部
Icnt, Decnt
Dir
215
コンテンツ蓄積部
217
218
Dlc
ライセンス情報処理部
Kd
コンテンツ復号部
Decnt
コンテンツ管理部214
Dtrn Dlc
Idva, Idvb
機器識別子格納部211
219
コンテンツ再生部
Drr Dir
伝送路31
音声出力

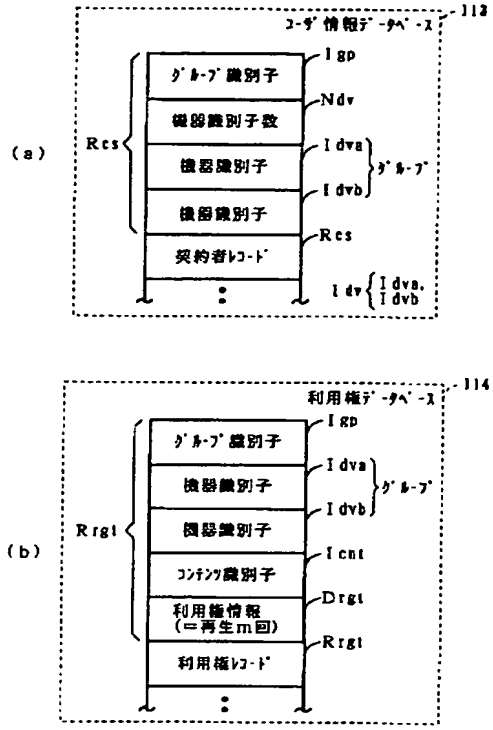
【図５】


217
ライセンス情報処理部
2172
ハッシュ値生成部
通信部 213
Dlc
2171
改竄判定部
Vlbs
Dlv
ハッシュ関数 f(x)
Dlc
2173
利用許可判定部
Ked
機器識別子格納部211
Idv
2174
復号鍵復号部
Kd
コンテンツ復号部218

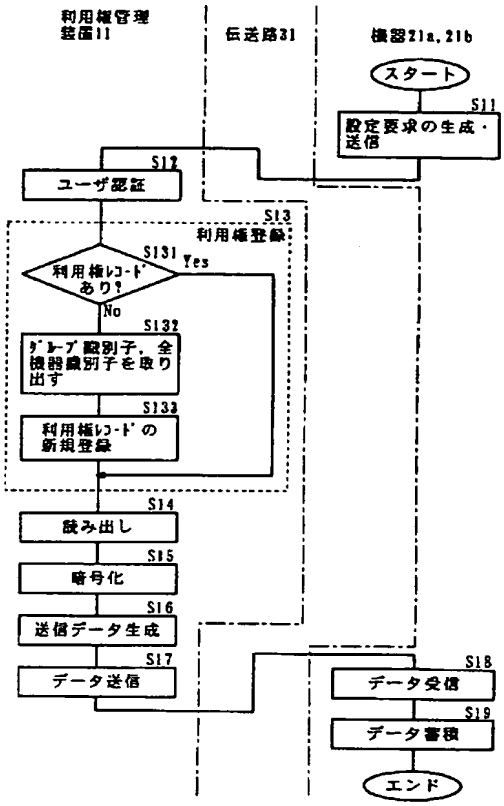
【図６】


(a)
111
コンテンツデータベース
コンテンツ識別子
Icnt
コンテンツデータ
Dcnt
暗号鍵
Ke
コンテンツ識別子
Icnt
コンテンツデータ
Dcnt
暗号鍵
Ke
(b)
112
復号鍵データベース
コンテンツ識別子
Icnt
復号鍵
Kd
コンテンツ識別子
Icnt
復号鍵
Kd

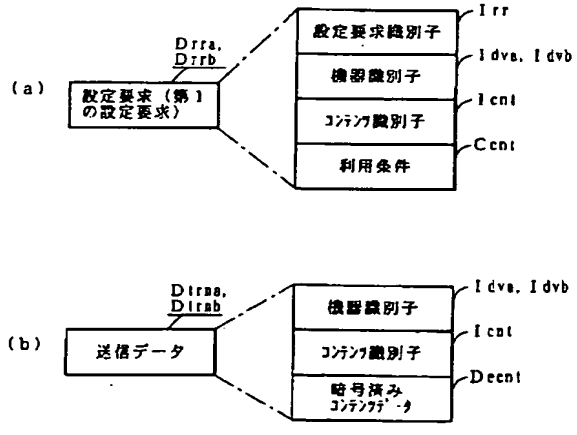
【図７】


(a)
ユーザ情報データベース
112
グループ識別子
機器識別子数
機器識別子
機器識別子
契約者レコード
Igp
Ndv
Idva
Idvb
グループ
Rcs
Idv {Idva, Idvb}
(b)
利用権データベース
114
グループ識別子
機器識別子
機器識別子
コンテンツ識別子
利用権情報
(＝再生m回)
利用権レコード
Igp
Idva
Idvb
グループ
Rrgt
Icnt
Drgt
Rrgt

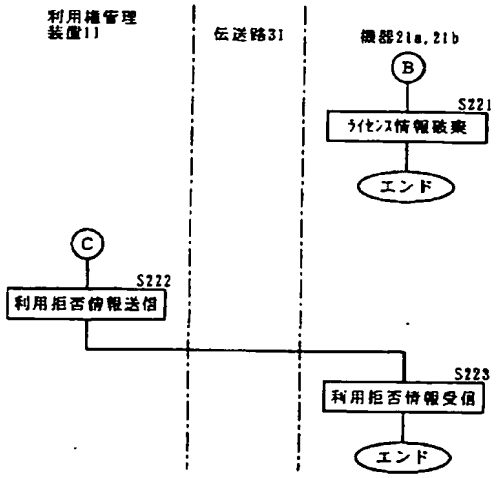
【図８】


利用権管理装置11
伝送路31
機器21a, 21b
スタート
S11
設定要求の生成・送信
S12
ユーザ認証
S13
利用権登録
S131
利用権レコードあり?
Yes
No
S132
グループ識別子，全機器識別子を取り出す
S133
利用権レコードの新規登録
S14
読み出し
S15
暗号化
S16
送信データ生成
S17
データ送信
S18
データ受信
S19
データ蓄積
エンド

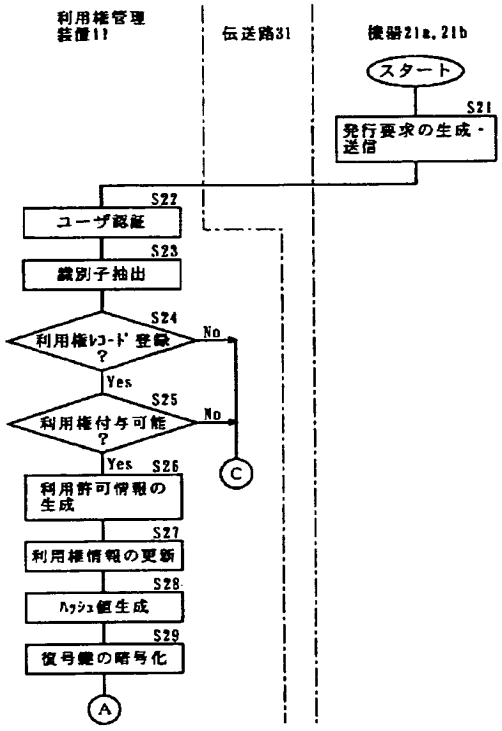
【図９】


(a)
設定要求（第1の設定要求）
Drra, Drrb
設定要求識別子
機器識別子
コンテンツ識別子
利用条件
Irr
Idva, Idvb
Icnt
Ccnt
(b)
送信データ
Dtrna, Dtrnb
機器識別子
コンテンツ識別子
暗号済みコンテンツデータ
Idva, Idvb
Icnt
Decnt

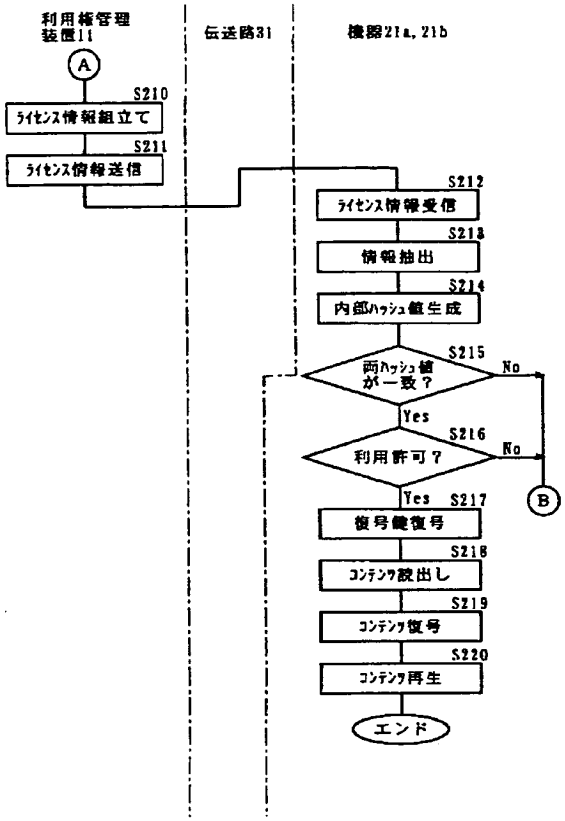
【図１３】


利用権管理装置11
伝送路31
機器21a, 21b
B
S221
ライセンス情報破棄
エンド
C
S222
利用拒否情報送信
S223
利用拒否情報受信
エンド

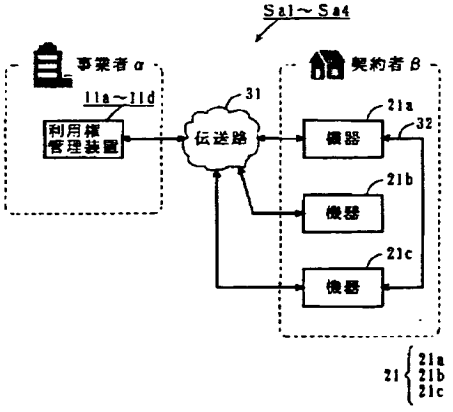
【図１１】



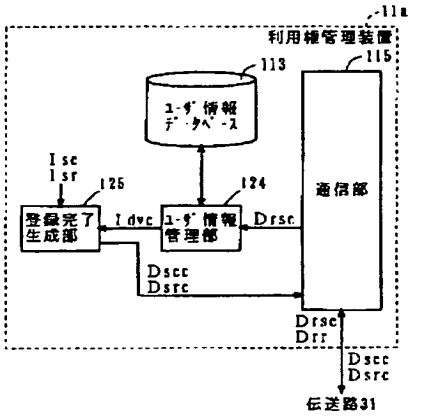
【図１２】



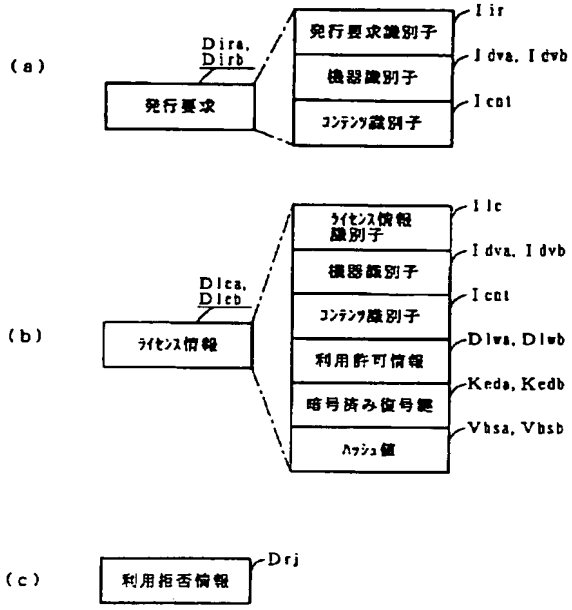
【図１５】



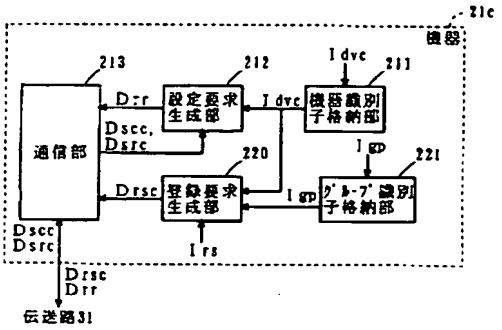
【図１６】



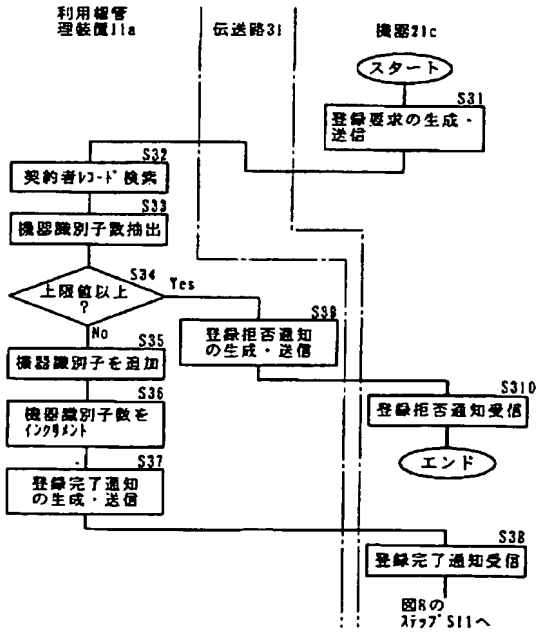
【図１４】



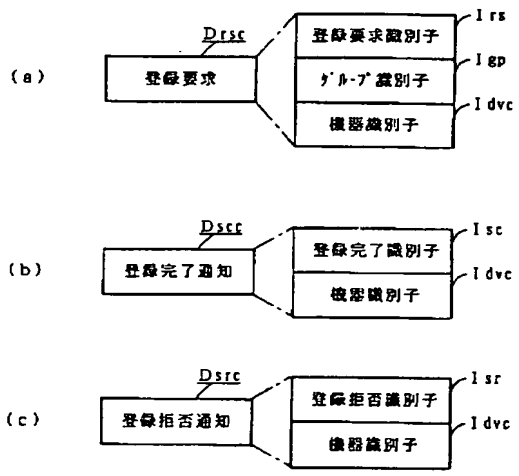
【図１７】



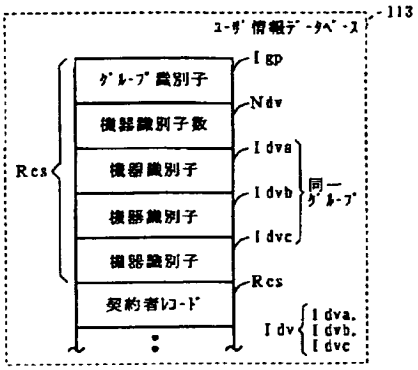
【図１８】



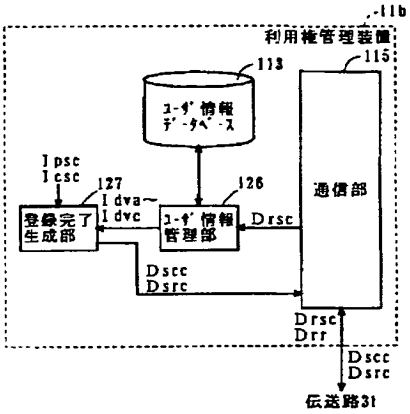
【図１９】



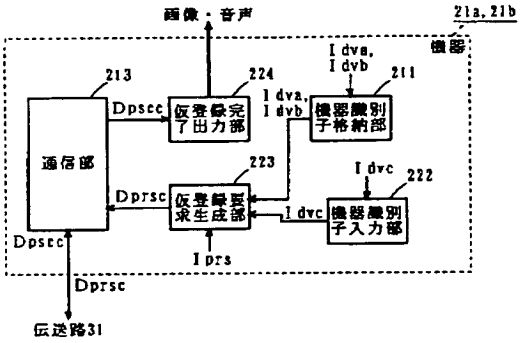
【図２０】



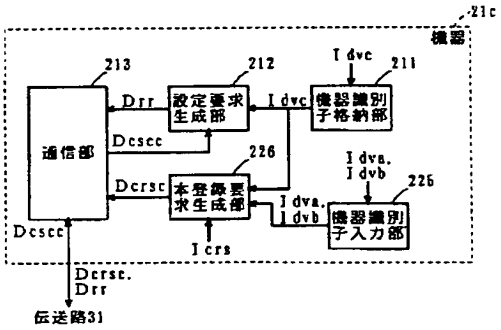
【図２１】



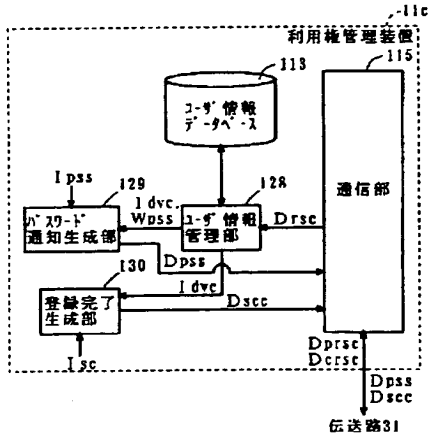
【図２２】



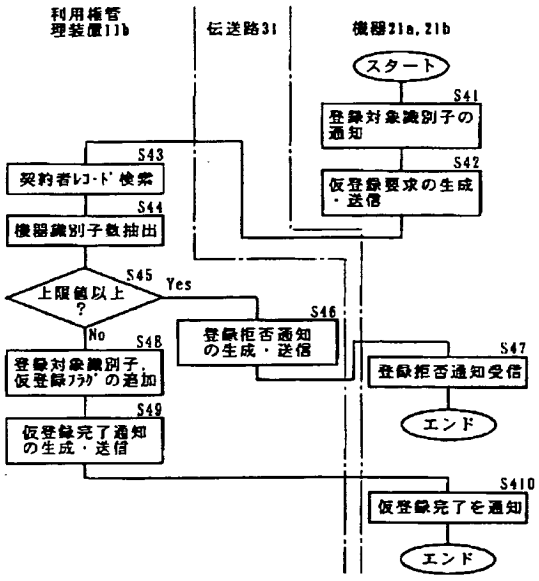
【図２３】



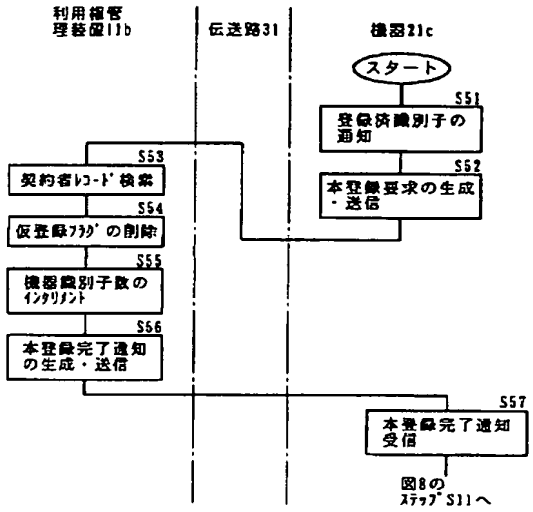
【図２９】



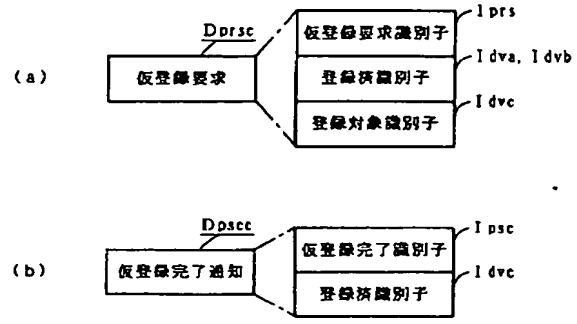
【図２４】



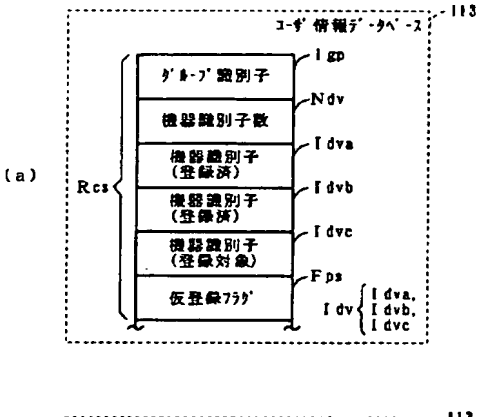
【図２５】

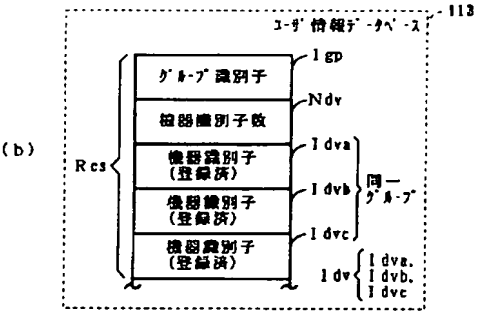


【図２６】

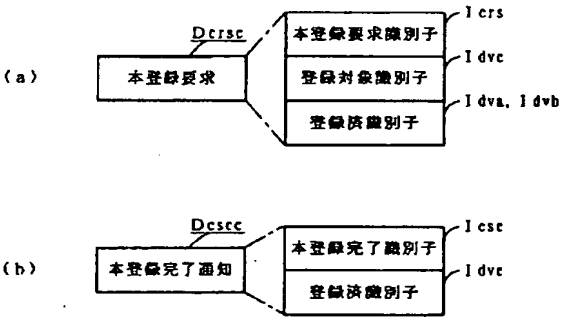


【図２７】

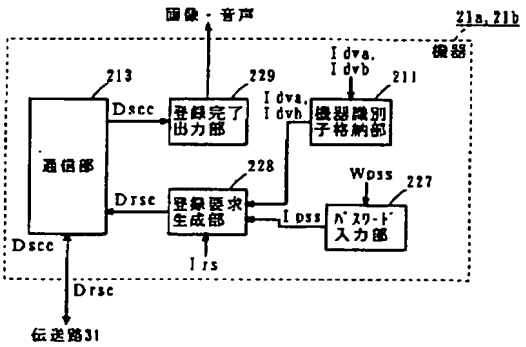




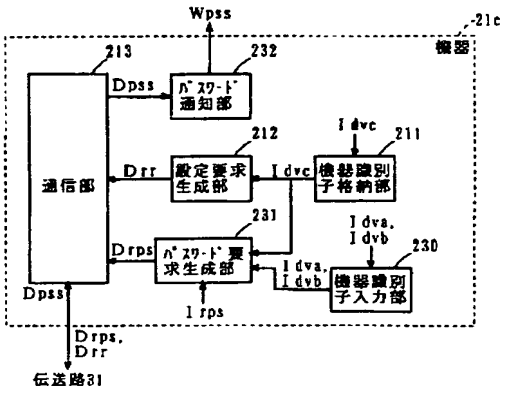
【図２８】



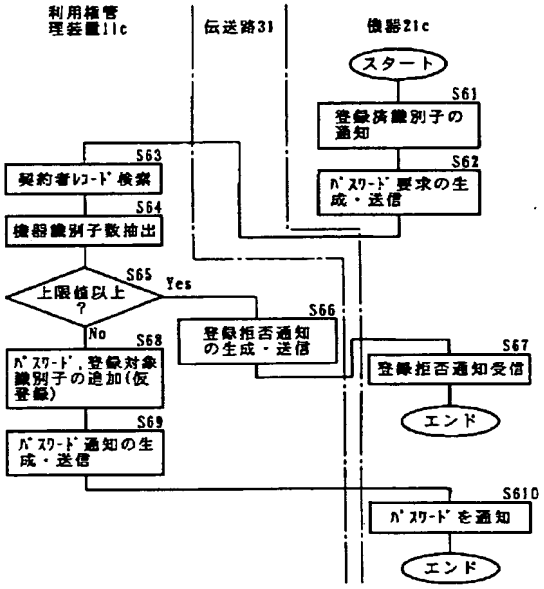
【図３０】



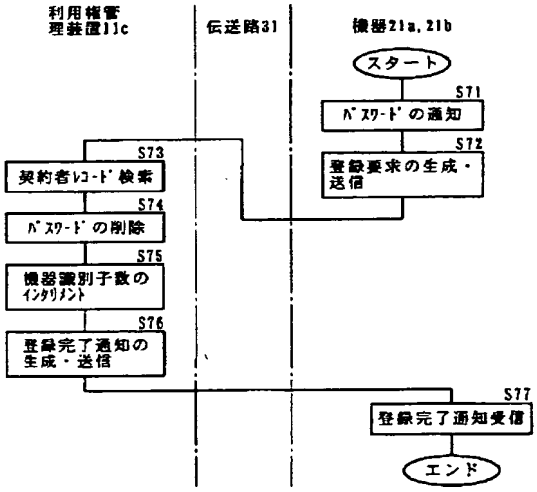
【図３１】



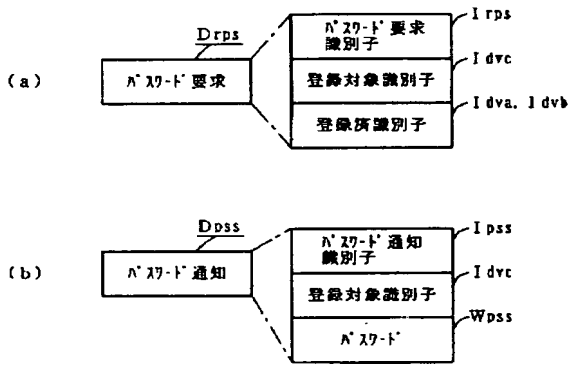
【図３２】



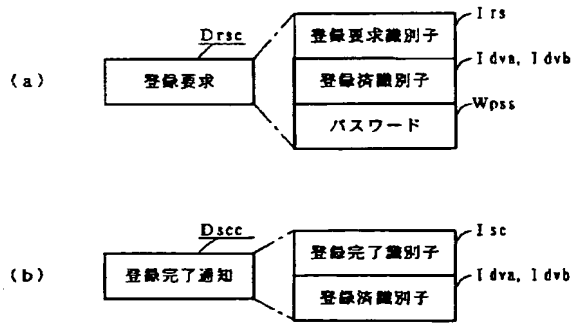
【図３３】



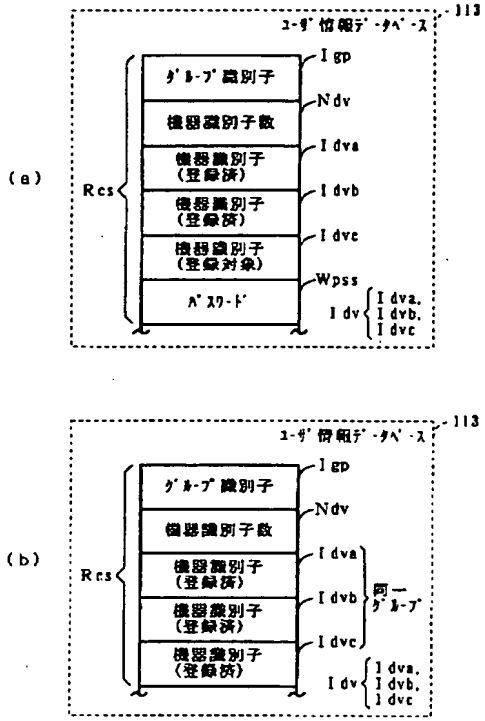
【図３４】



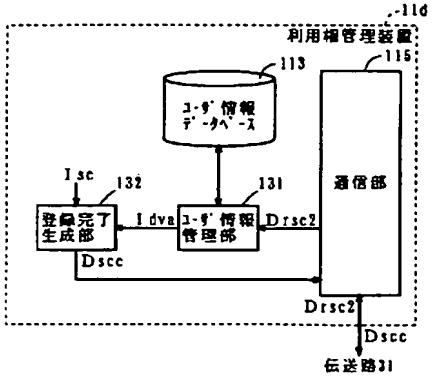
【図３６】



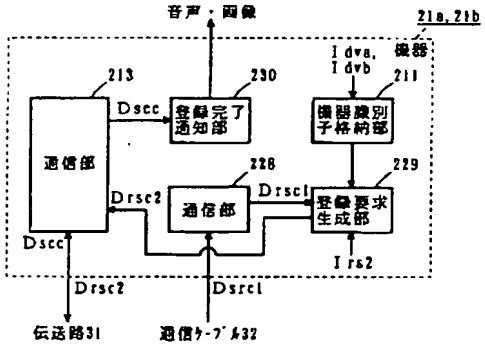
【図３５】



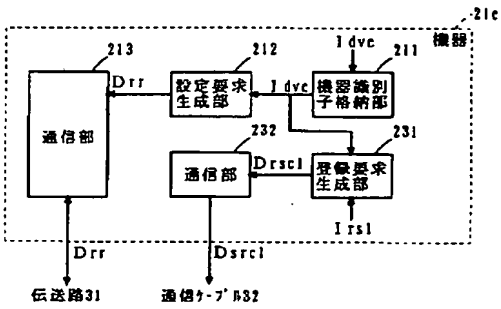
【図３７】



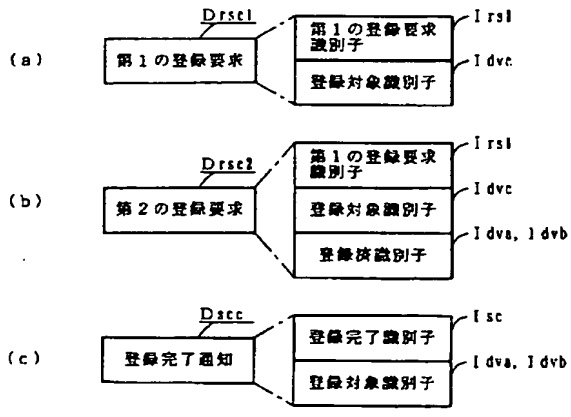
【図３８】



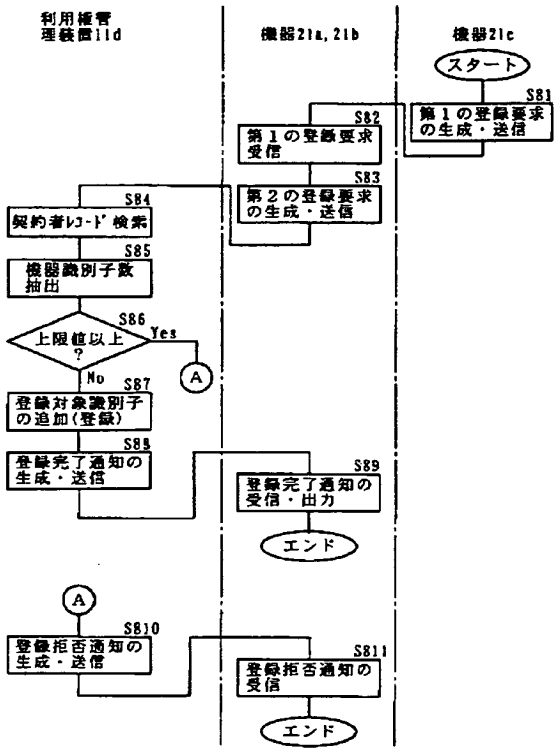
【図３９】



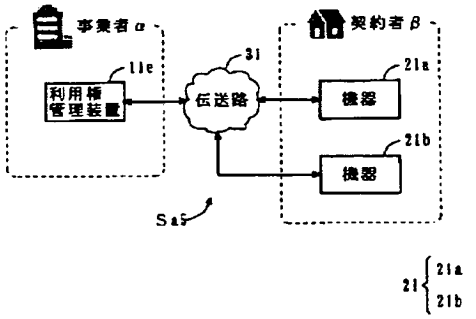
【図４１】



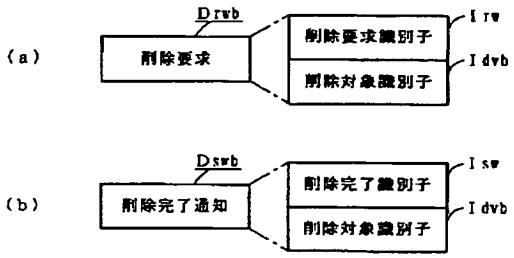
【図４０】



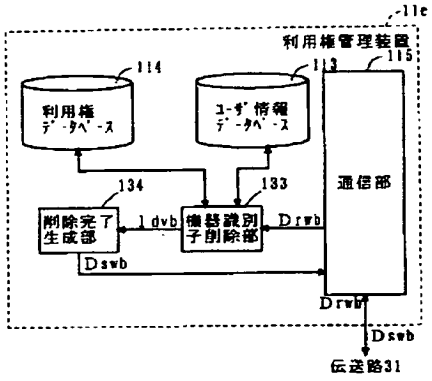
【図４２】



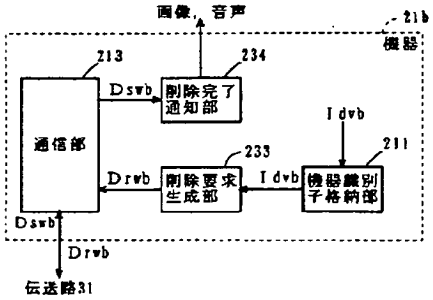
【図４６】



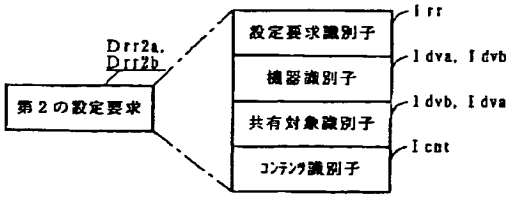
【図４３】



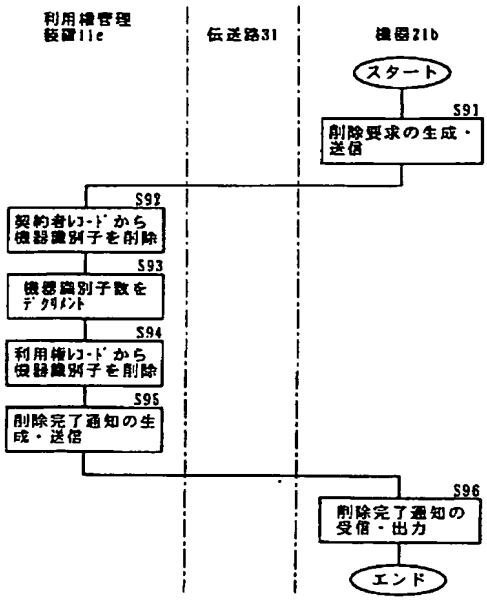
【図４４】



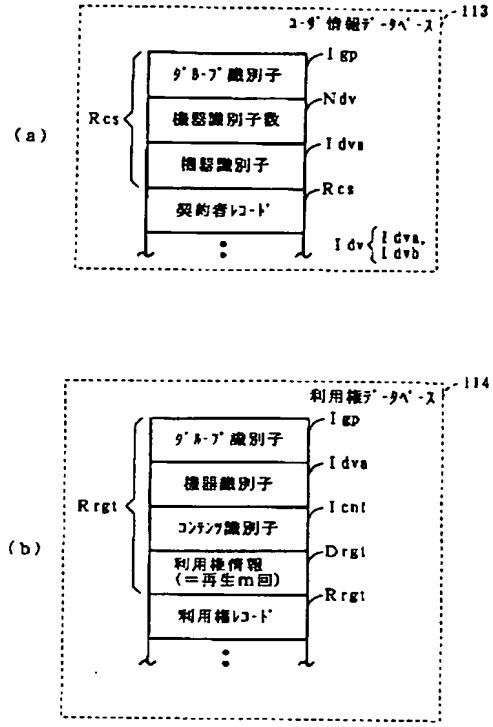
【図５３】



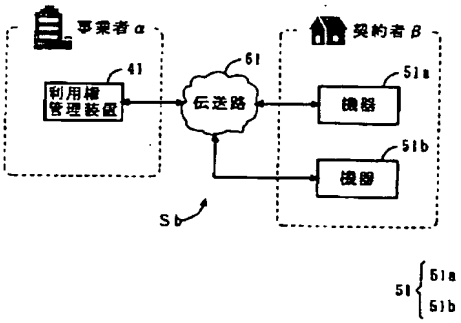
【図４５】



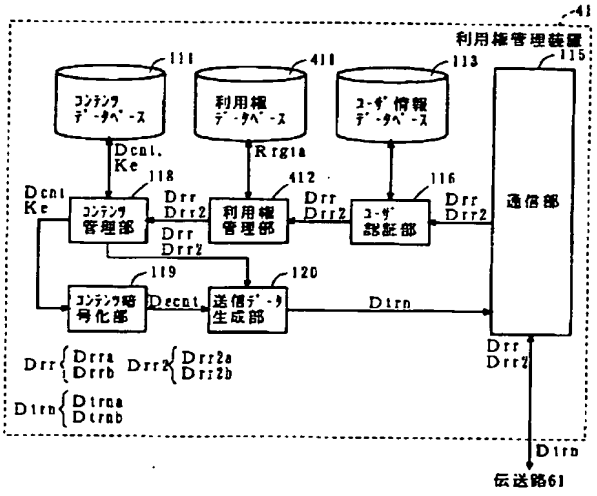
【図４７】



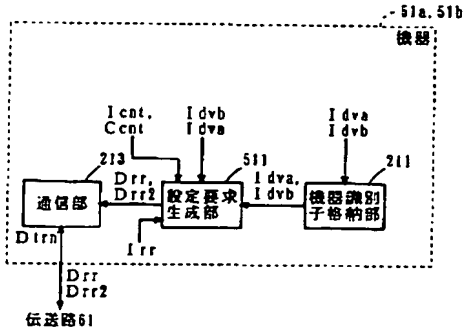
【図４８】



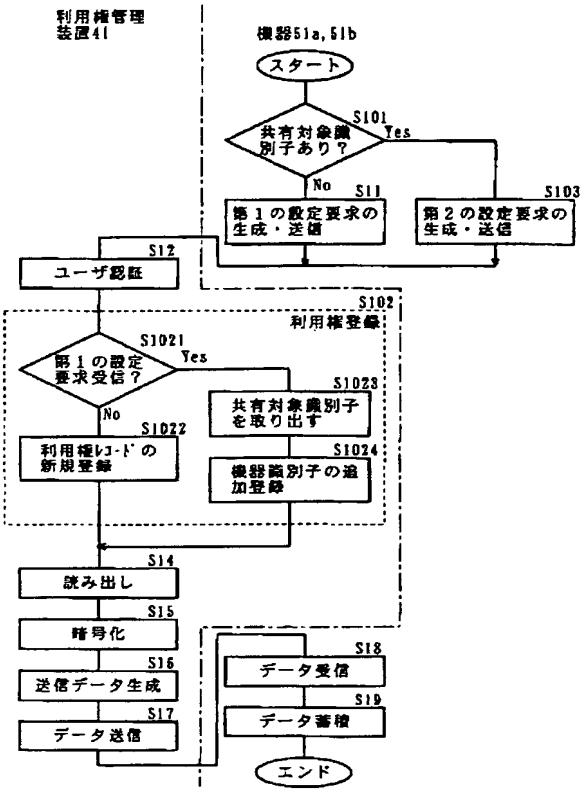
【図４９】



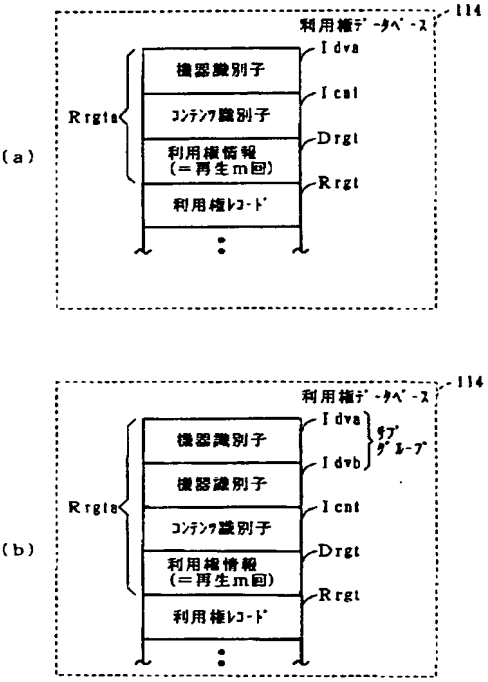
【図５０】



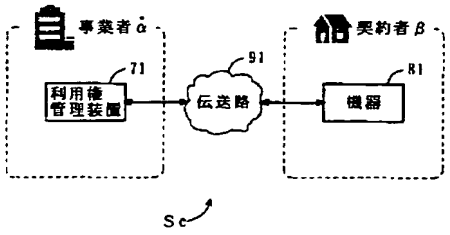
【図５１】



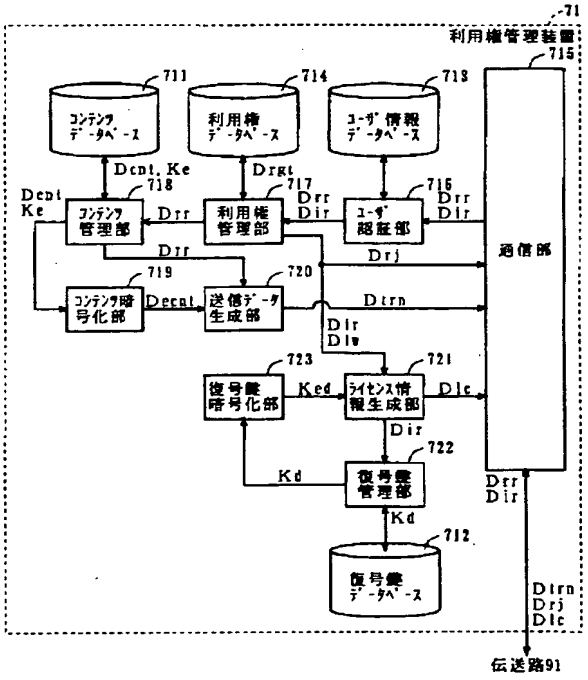
【図５２】



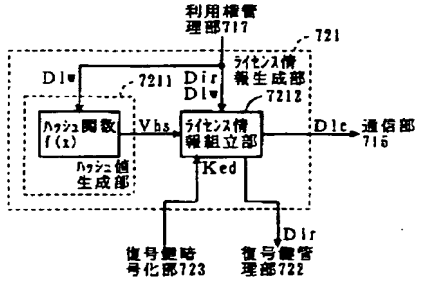
【図５４】



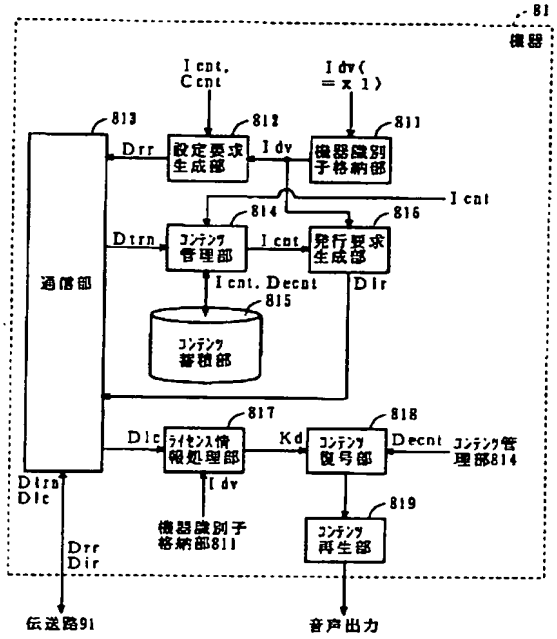
【図５５】



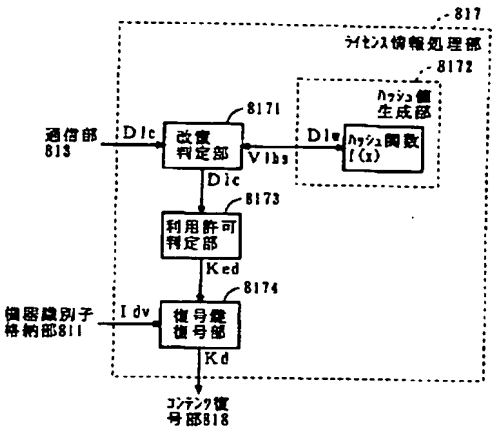
【図５６】



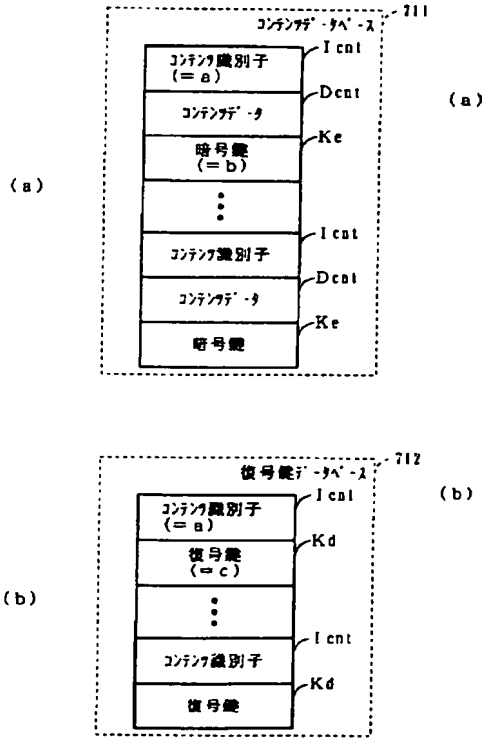
【図５７】



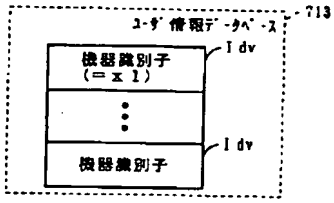
【図５８】

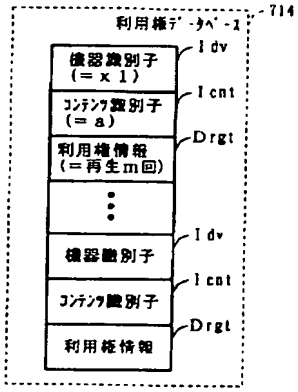


【図５９】

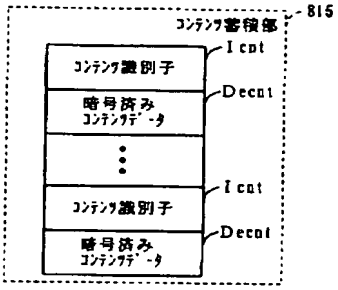


【図６０】

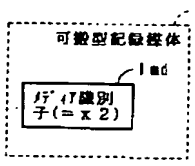




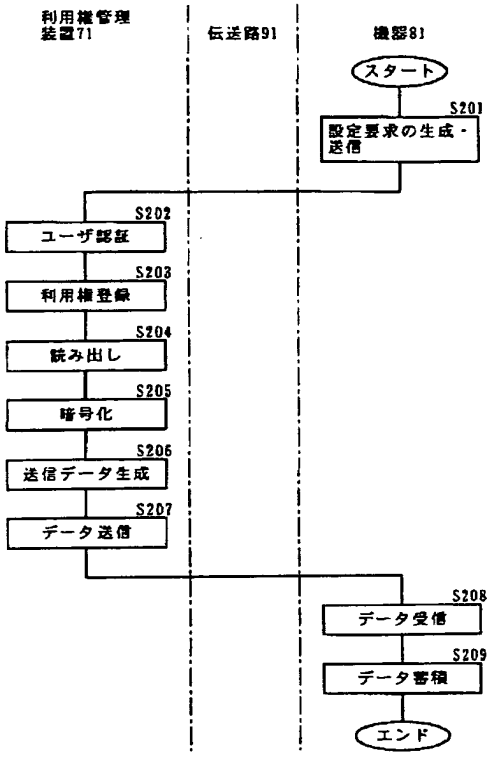
【図６３】



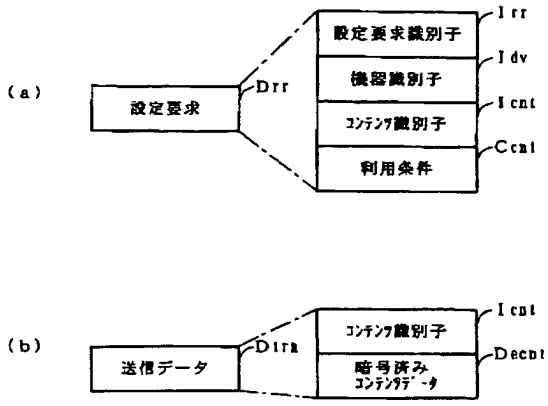
【図６９】



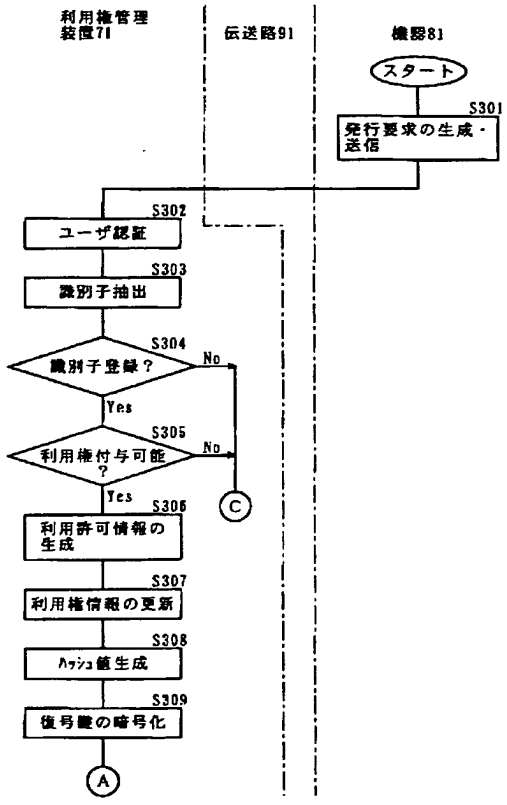
【図６１】



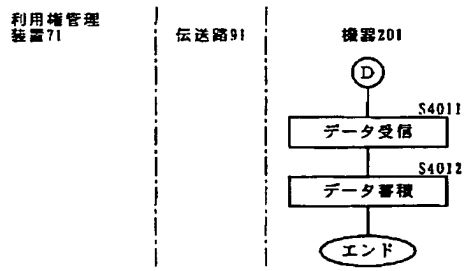
【図６２】



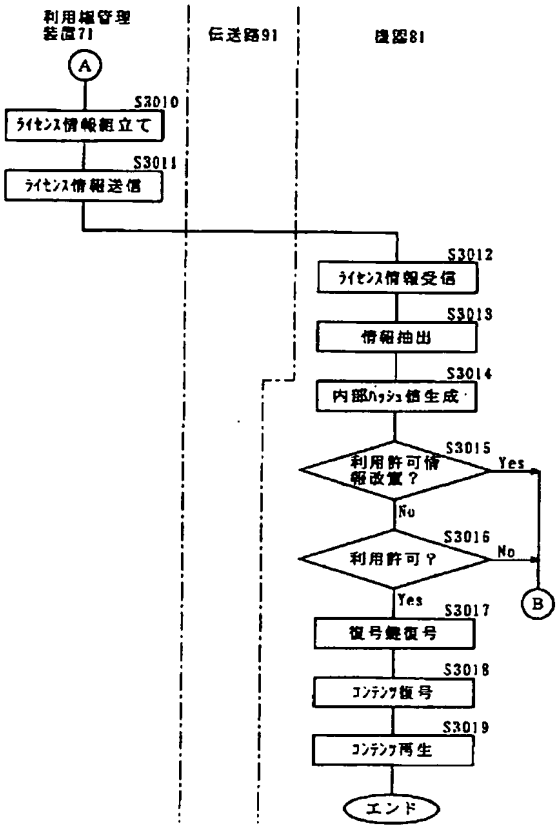
【図６４】



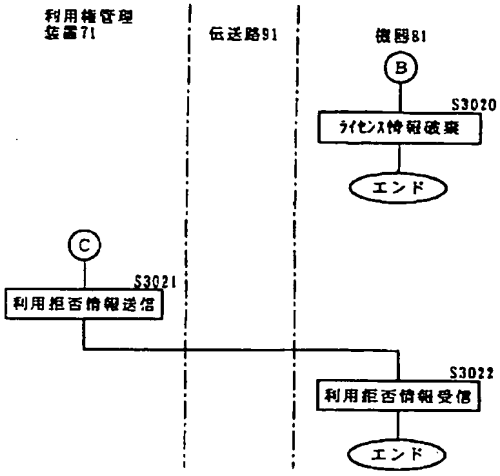
【図７３】



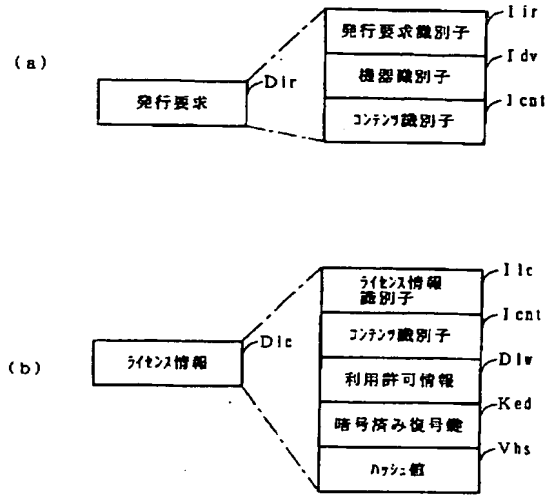
【図６５】



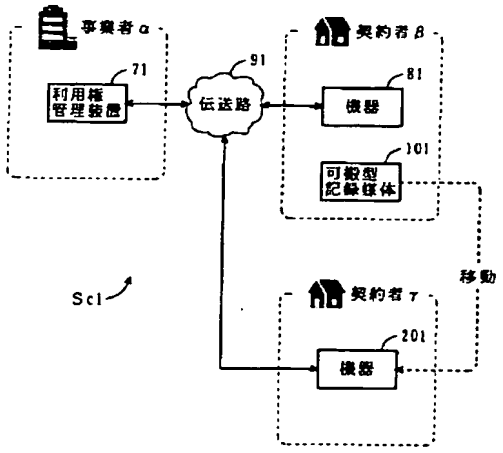
【図６６】



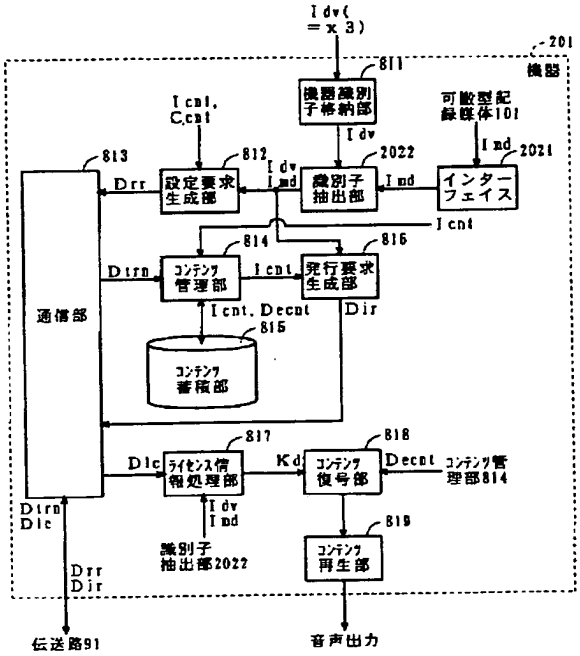
【図６７】



【図６８】

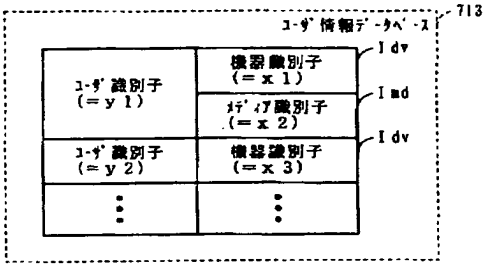


【図７０】

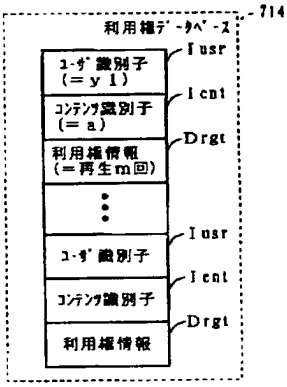


【図７１】

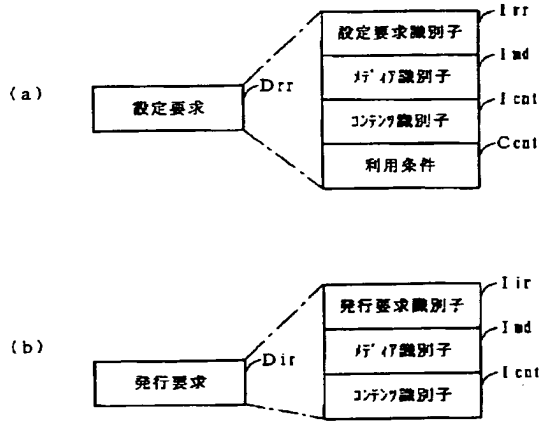
(a)



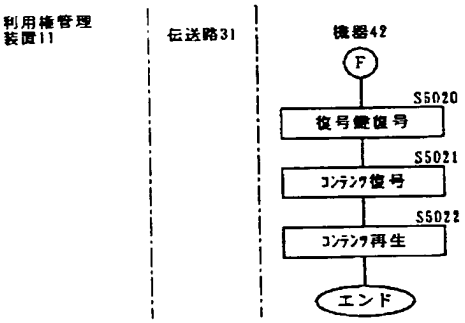
(b)



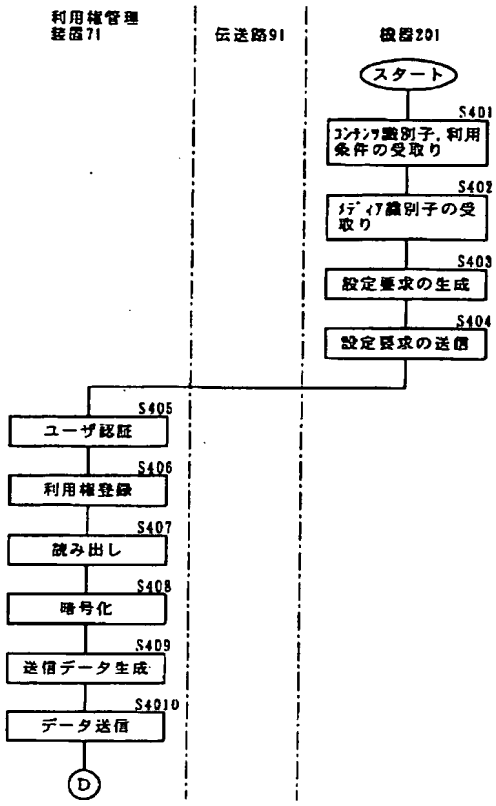
【図７４】



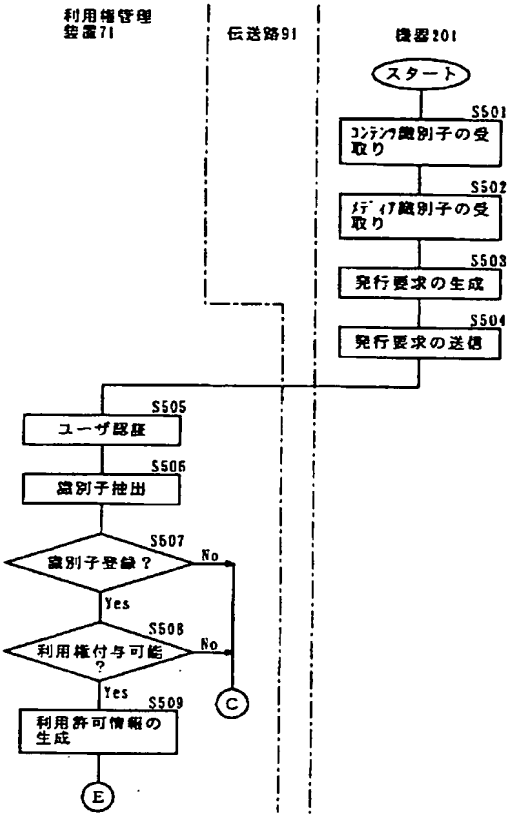
【図７７】



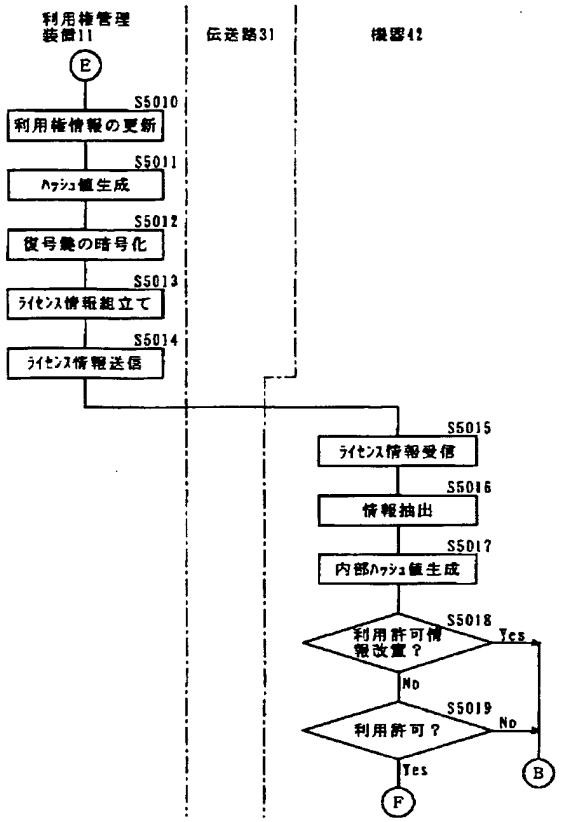
【図７２】


利用権管理装置71
伝送路91
機器201
スタート
S401
コンテンツ識別子，利用条件の受取り
S402
メディア識別子の受取り
S403
設定要求の生成
S404
設定要求の送信
S405
ユーザ認証
S406
利用権登録
S407
読み出し
S408
暗号化
S409
送信データ生成
S4010
データ送信
D

【図７５】


利用権管理装置71
伝送路91
機器201
スタート
S501
コンテンツ識別子の受取り
S502
メディア識別子の受取り
S503
発行要求の生成
S504
発行要求の送信
S505
ユーザ認証
S506
識別子抽出
S507
識別子登録？
No
Yes
S508
利用権付与可能？
No
Yes
C
S509
利用許可情報の生成
E

【図７６】



フロントページの続き

(51)Int.Cl.'	識別記号	F I		テーマコード（参考）
Ｈ０４Ｌ	9/08 9/32	Ｈ０４Ｌ	9/00	６０１Ｂ ６７３Ｂ

(72)発明者　山本　雅哉
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　岡本　隆一
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　徳田　克己
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　井上　光啓
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5B017 AA06 BB09 BB10 CA09 CA16
5B085 AE03 AE29 BA06 BG02 BG03
BG04 BG07
5J104 AA08 DA03 NA12 PA07 PA10